Réseaux informati

Nouvelle édition en français

Cisco CCNA

Guide de préparation à l'examen de certification CCNA 200-301

Volume 4

Sécurité et gestion du réseau

Cisco CCNA 200-301 Volume 4

Guide de préparation au Cisco CCNA 200-301 en français, Volume 4 Sécurité et gestion du réseau

François-Emmanuel Goffinet

Ce livre est en vente à http://leanpub.com/cisco-ccna-4

Version publiée le 2021-09-19

Aussi par François-Emmanuel Goffinet

Cisco CCNA 200-301 Volume 1

Cisco CCNA 200-301 Volume 2

Cisco CCNA 200-301 Volume 3

Linux Administration Volume 1

Linux Administration Volume 2

Linux Administration Volume 3

Linux Administration Volume 4

Protocole SIP

Table des matières

Avertissement

Le projet lié à cet ouvrage est conçu principalement pour des candidats francophones à l'examen de certification Cisco CCNA 200-301.

Le document sera probablement utile comme *support de formation* dans d'autres contextes tels que celui de l'autoapprentissage, de l'enseignement ou de la formation professionnelle.

Si le document peut sans doute contribuer à mieux connaître les réseaux d'entreprise dans la perspective du CCNA, il ne peut aucunement garantir la réussite de l'examen. Aussi, ce projet n'a jamais poursuivi l'ambition de remplacer d'autres sources d'information/formation issues des canaux officiels tels que *Cisco Press*, *Cisco Learning Network*, les *Cisco Systems Learning Partners*, *Cisco Academy* ou encore la documentation officielle du fabricant. D'ailleurs l'auteur est totalement indépendant de tout fabricant cité. Celles-ci, toutes mieux présentées les unes que les autres, ne manquent pas au contraire, mais il est rare de trouver des sources de qualité et fiables en français.

Copyrights

Dédicace

À mes parents qui m'ont toujours apporté un soutien sans faille dans tous mes projets.

Remerciements

Merci aux milliers de visiteurs quotidiens du site cisco.goffinet.org.

Merci aux centres de formation et aux écoles qui m'accordent leur confiance et qui me permettent de rencontrer mon public en personne.

Merci à Wendell Odom, mon mentor sur le sujet Cisco CCNA. N'hésitez pas à vous procurer ses livres en anglais chez Cisco Press.

Merci à Stéphane Bortzmeyer dont la prose prolifique m'inspire et m'aide à vulgariser les technologies de l'Internet.

Merci enfin à Cisco Systems d'être aussi ouvert depuis tant d'années dans sa documentation et pour son effort à rendre les technologies des réseaux plus accessibles, mieux comprises et plus populaires.

Avant-Propos

François-Emmanuel Goffinet est formateur IT et enseignant depuis 2002 en Belgique et en France. Outre Cisco CCNA, il couvre de nombreux domaines des infrastructures informatiques, du réseau à la virtualisation des systèmes, du nuage à la programmation d'infrastructures hétérogènes en ce y compris DevOps, Docker, K8s, chez AWS, GCP ou Azure, etc. avec une forte préférence et un profond respect pour l'Open Source, notamment pour Linux.

On trouvera ici un des résultats d'un projet d'autopublication en mode *agile* plus large lié au site web cisco.goffinet.org. La documentation devrait évoluer dans un format vidéo. Les sujets développés devraient trouver des questionnaires de validation de connaissances. Enfin, une solution accessible et abordable de simulation d'exercices pratiques mériterait réflexion.

Cisco CCNA 200-301

L'examen Cisco CCNA 200-301[1] est disponible en anglais uniquement. Il se déroule sous surveillance dans un centre de test VUE après une inscription sur leur site vue.com et un paiement (de maximum 300 EUR) avec un bon de réduction (*voucher*) ou par carte de crédit.

Cet examen de niveau fondamental sur la théorie des réseaux évalue votre niveau avec un examen sur ordinateur en anglais constitué d'une centaine de questions théoriques et pratiques. Cet examen a une durée de 120 minutes. Il est interdit de revenir sur une question à laquelle on a déjà répondu. Le seuil de réussite est fixé entre 82,5% et 85%. Tout diplômé d'un premier cycle de l'enseignement supérieur en informatique devrait être en mesure de réussir cet examen dans un délai de trois mois. Tout qui voudrait entrer dans une carrière dans les réseaux ne perd pas son temps en passant cet examen. Certains prétendent même que c'est fortement recommandé.

Sujets et objectifs de l'examen Cisco CCNA 200-301

On trouve 53 objectifs dans six sujets[2] : Fondamentaux des Réseaux (20%), Accès au Réseau (20%), Connectivité IP (25%), Services IP (10%), Sécurité de base (15%), Automation et Programmabilité (10%).

On trouve aussi dix verbes dans les objectifs de la certification CCNA 200-301 qui correspondent à certaines compétences à valider :

1. "Expliquer" (6)
2. "Décrire" (15)
3. "Comparer" (6)
4. "Identifier" (1)
5. "Reconnaître" (1)
6. "Interpréter" (2)
7. "Déterminer" (1)
8. "Définir" (1)
9. "Configurer" (17)
10. "Vérifier" (1)

On peut considérer que seuls les objectifs qui demandent à "Configurer" et à "Vérifier" seraient purement pratiques. Toutefois, "Identifier", "Interpréter" et "Déterminer" pourraient aussi trouver leur application opérationnelle. Les autres objectifs comme "Expliquer", "Décrire", "Définir", "Reconnaître" seraient validés par des questions d'examen plus théoriques.

Les objectifs développés dans ce volume sont indiqués en gras.

1. La page officielle de la certification se trouve à cette adresse.
2. La page officielle des sujets et des objectifs du Cisco CCNA 200-301 se trouve à cette adresse.

1.0 Fondamentaux des Réseaux - 20%

- 1.1 Expliquer le rôle et la fonction des composants réseau
  - 1.1.a Routeurs
  - 1.1.b Commutateurs (switches) L2 et L3
  - 1.1.c Pare-feu NG (Next-generation firewalls) et IPS
  - 1.1.d Point d'accès (Access points)
  - 1.1.e Controlleurs (Cisco DNA Center et WLC)
  - 1.1.f Points terminaux (Endpoints)
  - 1.1.g Serveurs
- 1.2 Décrire les caractéristiques des architectures et topologies réseau
  - 1.2.a 2 tier
  - 1.2.b 3 tier
  - 1.2.c Spine-leaf
  - 1.2.d WAN
  - 1.2.e Small office/home office (SOHO)
  - 1.2.f On-premises et cloud
- 1.3 Comparer les interfaces physiques et les types de câble
  - 1.3.a Fibre monmode (Single-mode) et fibre multimode, cuivre
  - 1.3.b Connexions (Ethernet shared media et point-to-point)
  - 1.3.c Concepts sur PoE
- 1.4 Identifier les problèmes d'interface et de câbles (collisions, errors, mismatch duplex, et/ou speed)
- 1.5 Comparer TCP à UDP
- 1.6 Configurer et vérifier l'adressage et le sous-réseautage (subnetting) IPv4
- 1.7 Décrire la nécessité d'un adressage IPv4 privé
- 1.8 Configurer et vérifier l'adressage et les préfixes IPv6
- 1.9 Comparer les types d'adresses IPv6
  - 1.9.a Global unicast
  - 1.9.b Unique local
  - 1.9.c Link local
  - 1.9.d Anycast
  - 1.9.e Multicast
  - 1.9.f Modified EUI 64
- 1.10 Vérifier les paramètres IP des OS clients (Windows, Mac OS, Linux)
- 1.11 Décrire les principes des réseaux sans-fil
  - 1.11.a Nonoverlapping Wi-Fi channels
  - 1.11.b SSID
  - 1.11.c RF
  - 1.11.d Encryption
- 1.12 Expliquer les fondamentaux de la virtualisation (virtual machines)
- 1.13 Décrire les concepts de la commutation (switching)
  - 1.13.a MAC learning et aging
  - 1.13.b Frame switching
  - 1.13.c Frame flooding
  - 1.13.d MAC address table

2.0 Accès au Réseau - 20%

- 2.1 Configurer et vérifier les VLANs (normal range) couvrant plusieurs switches
  - 2.1.a Access ports (data et voice)
  - 2.1.b Default VLAN
  - 2.1.c Connectivity
- 2.2 Configurer et vérifier la connectivité interswitch
  - 2.2.a Trunk ports
  - 2.2.b 802.1Q
  - 2.2.c Native VLAN
- 2.3 Configurer et vérifier les protocoles de découverte Layer 2 (Cisco Discovery Protocol et LLDP)
- 2.4 Configurer et vérifier (Layer 2/Layer 3) EtherChannel (LACP)
- 2.5 Décrire la nécessité et les operations de base de Rapid PVST+ Spanning Tree Protocol
  - 2.5.a Root port, root bridge (primary/secondary), et les autres noms de port
  - 2.5.b Port states (forwarding/blocking)
  - 2.5.c Avantages PortFast
- 2.6 Comparer les architectures Cisco Wireless Architectures et les modes des APs
- 2.7 Décrire les connexions physiques d'infrastructure des composants WLAN (AP,WLC, access/trunk ports, et LAG)
- 2.8 Décrire les connexions des accès de gestion des APs et du WLC (Telnet, SSH, HTTP,HTTPS, console, et TACACS+/RADIUS)
- 2.9 Configurer les composants d'un accès au LAN sans-fil pour la connectivité d'un client en utilisant un GUI seulement pour la création du WLAN, les paramètres de sécurité, les profiles QoS et des paramètres WLAN avancés

3.0 Connectivité IP - 25%

- 3.1 Interpréter les composants d'une table de routage
  - 3.1.a Routing protocol code
  - 3.1.b Prefix
  - 3.1.c Network mask
  - 3.1.d Next hop
  - 3.1.e Administrative distance
  - 3.1.f Metric
  - 3.1.g Gateway of last resort
- 3.2 Déterminer comment un routeur prend une décision de transfert par défaut
  - 3.2.a Longest match
  - 3.2.b Administrative distance
  - 3.2.c Routing protocol metric
- 3.3 Configurer et vérifier le routage statique IPv4 et IPv6
  - 3.3.a Default route
  - 3.3.b Network route

  - 3.3.c Host route
  - 3.3.d Floating static

- 3.4 Configurer et vérifier single area OSPFv2
  - 3.4.a Neighbor adjacencies
  - 3.4.b Point-to-point
  - 3.4.c Broadcast (DR/BDR selection)
  - 3.4.d Router ID

- 3.5 Décrire le but des protocoles de redondance du premier saut (first hop redundancy protocol)

4.0 Services IP - 10%

- 4.1 Configurer et vérifier inside source NAT (static et pools)
- 4.2 Configurer et vérifier NTP dans le mode client et le mode server
- 4.3 Expliquer le rôle de DHCP et de DNS au sein du réseau
- 4.4 Expliquer la fonction de SNMP dans les opérations réseau
- 4.5 Décrire l'utilisation des fonctionnalités de syslog features en ce inclus les facilities et niveaux
- 4.6 Configurer et vérifier DHCP client et relay
- 4.7 Expliquer le forwarding per-hop behavior (PHB) pour QoS comme classification, marking, queuing, congestion, policing, shaping
- 4.8 Configurer les périphériques pour un accès distant avec SSH
- 4.9 Décrire les capacités la fonction de TFTP/FTP dans un réseau

5.0 Sécurité de base - 15%

- 5.1 Définir les concepts clé de la sécurité (menaces, vulnerabilités, exploits, et les techniques d'atténuation)
- 5.2 Décrire les éléments des programmes de sécurité (sensibilisation des utilisateurs, formation, le contrôle d'accès physique)
- 5.3 Configurer l'accès aux périphériques avec des mots de passe
- 5.4 Décrire les éléments des politiques de sécurité comme la gestion, la complexité, et les alternatives aux mots de passe (authentications multifacteur, par certificats, et biométriques)
- 5.5 Décrire les VPNs remote access et site-to-site
- 5.6 Configurer et vérifier les access control lists
- 5.7 Configurer les fonctionnalités de sécurité Layer 2 (DHCP snooping, dynamic ARP inspection, et port security)
- 5.8 Distinguer les concepts authentication, authorization, et accounting
- 5.9 Décrire les protocoles de sécurité sans-fil (WPA, WPA2, et WPA3)
- 5.10 Configurer un WLAN en utilisant WPA2 PSK avec un GUI

6.0 Automation et Programmabilité - 10%

- 6.1 Expliquer comment l'automation impacte la gestion du réseau
- 6.2 Comparer les réseaux traditionnels avec le réseau basé contrôleur (controller-based)
- 6.3 Décrire les architectures basées contrôleur (controller-based) et software defined (overlay, underlay, et fabric)
  - 6.3.a Séparation du control plane et du data plane
  - 6.3.b APIs North-bound et south-bound
- 6.4 Comparer la gestion traditionnelle les périphériques campus avec une gestion des périphériques avec Cisco DNA Center
- 6.5 Décrire les caractéristiques des APIs de type REST (CRUD, verbes HTTP, et encodage des données)
- 6.6 Reconnaître les capacités des mécanismes de gestion des configuration comme Puppet, Chef, et Ansible
- 6.7 Interpréter des données encodées en JSON

Introduction

Ce quatrième et dernier volume du guide de préparation à la certification Cisco CCNA 200-301 est l'ultime étape dans votre projet de formation. Il complète le propos de l'examen sur des sujets comme la sécurité dans le réseau local, le pare-feu, les tunnels VPN, les protocoles de gestion comme NTP, Syslog, SNMP, la gestion sécurisée des périphériques ainsi que les rudiments de programmabilité des réseaux. L'ouvrage couvre les sujets suivants de la certification CCNA : Sécurité de base et Automation et Programmabilité.

Ce volume peut occuper une activité intellectuelle de 16 à 35 heures, voir plus.

L'objectif opérationnel est de concevoir une architecture réseau agile et sécurisée.

La première partie invite à prendre conscience de l'ampleur des menaces sur le réseau local et à envisager les contre-mesures disponibles et les bonnes pratiques particulièrement sur le matériel Cisco Systems. On apprendra à mettre en place une mesure de sécurité de type Port-Security qui vise à limiter le nombre d'adresses MAC qui peuvent se connecter à un port de commutateur, mais aussi les sécurité Deep ARP Inspection (DAI) et DHCP Snooping.

Dans la seconde partie, on évoquera des pratiques de gestion sécurisée comme la configuration des consoles distantes (Telnet, SSH) et locales, le transfert de fichiers (TFTP, FTP, SCP) et la vérification de fichiers (MD5). On parlera aussi de différents protocoles ou solutions que les utilisateurs finaux ignorent, car ils n'en ont pas besoin, mais qui sont utiles à la gestion et la surveillance du réseau (CDP, LLDP, SYSLOG, NTP, SNMP).

La troisième partie porte sur l'automation et la programmabilité du réseau : sur les architectures contrôlées de type SDN, sur le concept d'Intent Based Network, d'automation et d'outils d'automation. Enfin, on terminera le propose sur le protocole HTTP, les actions CRUD, la manipulation d'APIs HTTP REST et le traitement des sorties en format de présentation JSON.

Les trois parties suivantes visent à démontrer en théorie et en pratiques les concepts de pare-feu/IDS et de tunnels VPN IPSEC site à site.

Enfin, l'ouvrage se termine par une partie récapitulative des sujets de la certification Cisco CCNA.

Première partie Sécurité dans le LAN

Le réseau local, le LAN comme on l'appelle communément, est constitué principalement de commutateurs et/ou de commutateurs multi-couches (L2/L3), et si il y a du Wi-fi, on trouvera des contrôleurs de points-d'accès et d'antennes WLAN qui offrent l'accès au réseau et à ses services pour les utilisateurs. Cette partie de l'infrastructure de communication est particulièrement délaissée en terme de sécurité et d'audit au profit de l'historique pare-feu qui, on le rappellera, filtre les flux de trafic qui le traverse. Il n'intervient que très peu au sein du réseau local, sauf sur les hôtes terminaux. Alors que celui-ci placé en bordure du réseau empêche toute intrusion directe de l'extérieur du LAN, il contrôle aussi le trafic sortant, notamment celui-ci des utilisateurs. Très bien, mais qu'en est-il de la confidentialité, de l'authentification et de l'intégrité des messages utilisateurs à partir du réseau local ?

Dans un premier temps, on tentera de prendre conscience de l'ampleur des menaces sur le réseau local et d'envisager les contre-mesures disponibles particulièrement sur le matériel Cisco Systems. Ensuite, on envisagera d'illustrer ces menaces dans un exercice de laboratoire uniquement prévu à cet effet. Enfin, on ne manquera pas de parler du sujet de l'authentification sur les ports d'accès filaire ou non comme IEEE 802.1X/EAP/Radius.

On apprendra aussi à mettre en place une mesure de sécurité de type "Port-Security" qui vise à limiter le nombre d'adresse MAC qui peuvent se connecter à un port de commutateur. Cette mesure permet de contrôler le trafic au plus bas niveau de la connectivité, au plus proche du trafic des utilisateurs. Réalisant un filtrage au plus bas niveau avec une souplesse de gestion limitée, la facilité "Port-Security" pourrait provoquer des effets indésirables de faux positifs. Elle ne se déploie donc pas à la légère quand bien même cette compétence est fortement vérifiée dans la certification Cisco CCNA.

1. Introduction à la sécurité dans le LAN

1. Introduction à la sécurité des systèmes d'information

1.1. Objectifs de la sécurité des systèmes d'information

La sécurité des systèmes d'information vise les objectifs suivants (CIA)[1] :

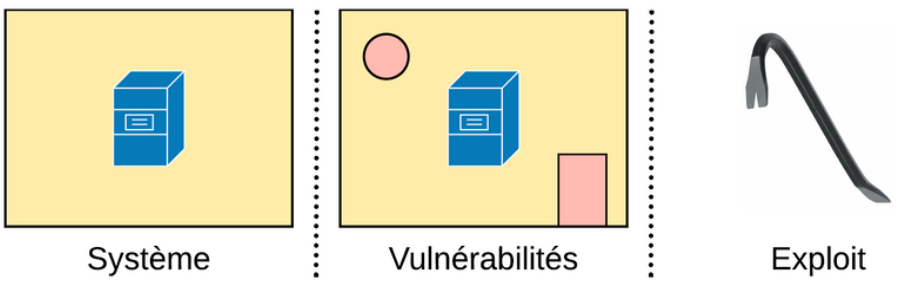
- La **confidentialité** : Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.
- L'**intégrité** : Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.
- La **disponibilité** : Le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

D'autres aspects de "preuve" peuvent aussi être considérés comme des objectifs de la sécurité des systèmes d'information, tels que :

- L'**authentification** : L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.
- La **non-répudiation** et l'**imputation** : Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.
- La **traçabilité** (ou « **Preuve** ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

1.2. Vulnérabilités

Tous les actifs d'un système d'information peuvent faire l'objet de **vulnérabilités**, soit d'une **faiblesse** qui pourrait compromettre un critère de sécurité défini comme l'accès non autorisé à des données confidentielles ou la modification d'un système. Un **exploit** est une charge informatique ou un outil qui permet d'"exploiter" une faiblesse ciblée, soit une vulnérabilité.



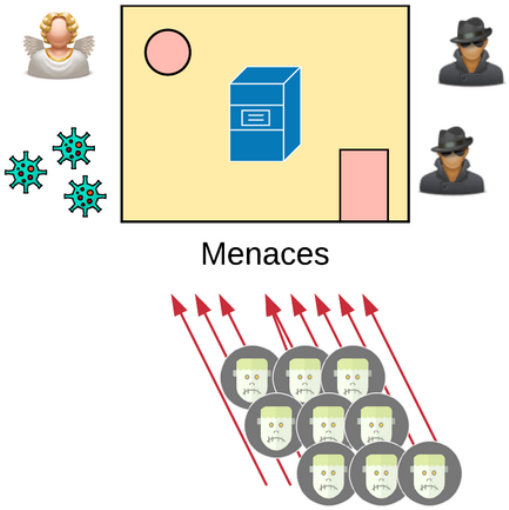
Vulnérabilités des systèmes et exploits

1. Sécurité des systèmes d'information, Objectifs.

1.3. Menaces

Une menace est l'action probable qu'une personne malveillante puisse mener grâce à un "exploit" contre une faiblesse en vue d'atteindre à sa sécurité. Une menace est une cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation. Quelques exemples de menaces courantes :

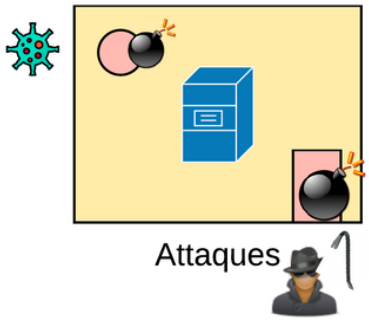
- Code malveillant
- Personnes extérieures malveillantes
- Perte de service
- Stagiaire malintentionné



Menaces sur les systèmes

1.4. Attaques

Une attaque est l'action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la concrétisation d'une menace nécessitant l'exploitation d'une vulnérabilité.



Attaques sur les systèmes

1.5. Risques

Une fois les objectifs de sécurisation déterminés, les risques d'attaque pesant sur chacun de ces éléments peuvent être estimés en fonction de **menaces** et de vulnérabilités.

Le niveau global de sécurité des systèmes d'information est défini par le niveau de sécurité du maillon le plus faible. Les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

Il faudrait pour cela estimer :

- la *gravité* des impacts au cas où les risques se réaliseraient,
- la *vraisemblance* des risques (ou leur *potentialité*, ou encore leur *probabilité d'occurrence*).

1.6. Vecteurs d'attaque

1.7. Perte et fuite de données

data loss prevention (DLP)

1.8. Outils de Pentest

3. Typologie des attaques

- Usurpation d'adresses (Spoofing)
- Attaque de reconnaissance
- Eavesdropping attack
- Attaque Buffer Overflow
- Malwares
- Vulnérabilités humaines
- Vulnérabilités des mots de passe

3.1 Usurpation d'adresses (Spoofing)

3.2. Attaque Denial-of-Service (DoS)/(DDoS)

3.3. Attaque par réflexion

3.4. Attaque par amplification

3.5. Attaque Man-in-the-Middle (MitM)

3.6. Attaque de reconnaissance

Attaque d'accès

3.7. Eavesdropping attack

3.8. Attaque Buffer Overflow

3.9. Types de Malwares

Trojan, Virus, Vers

3.10. Vulnérabilités humaines

Voici un jargon d'ingéniérie sociale :

- Social engineering : Exploite la crédulité et la confiance humaine ainsi que les comportements sociaux.
- Phishing : Dégise une invitation malveillante en quelque chose de légitime.
- Spear phishing : Cible un groupe d'utilisateurs semblables.
- Whaling : Cible des profil individuels de haut-niveau.
- Vishing : Utilise des messages vocaux.
- Smishing : Utilise des messages texte SMS.
- Pharming : Utilise des services légitimes pour envoyer des utilisateurs vers un site compromis.
- Watering hole : Cible des victimes spécifiques vers un site compromis.

3.11. Vulnérabilités des mots de passe

3.12. Attaques IP

3.14. Attaques TCP

2. Sécurité dans le LAN

2.1. Introduction

On trouvera énormément de vulnérabilités intrinsèques dans le réseau LAN pour une raison simple : les administrateurs partent du principe de confiance. Tout accès au LAN est cédé aux utilisateurs par un contrat de confiance dont la limite est l'abus de la crédulité des solutions mises en place dans l'infrastructure.

On en pensera ce que l'on voudra. Toutefois cela ne nous empêche certainement pas de nous poser quelques questions sur le sujet. Quelle sont ces vulnérabilités que l'on peut rencontrer dans un LAN ? Quels sont les cibles et les attaques potentielles ? Et, enfin, quelles sont les bonnes pratiques et les remèdes à appliquer ?

2.2. Attaques

On trouvera quasiment toute la terminologie des attaques dans le domaine de la sécurité des infrastructures de réseaux locaux qui rompent les principes fondamentaux de confidentialité, d'intégrité et d'authentification : écoute, usurpation, déni de service (DoS), MitM (homme du milieu, Man-in-the Middle), …

Les vecteurs d'attaques sont des humains qui ont des accès autorisés ou non au réseau, mais aussi des logiciels malveillants pilotés automatiquement ou à distance. Dès qu'un accès au réseau local est compromis, la plupart du temps, la porte est ouverte sur les services du système d'information de l'organisation.

Si les attaques de déni de service (DoS) sont parmi les plus crapuleuses et les moins intéressantes, elles seraient néanmoins les plus visibles et les plus faciles à mettre en oeuvre avec peu de moyens de réaction du côté des défenseurs. Ces dernières sont donc aussi des menaces sur le LAN à prendre en compte.

2.3. Cibles

Toute technologie d'accès comme Ethernet ou Wi-Fi sur le LAN (ou le "WLAN", mais aussi les réseaux mobiles) sont touchés par cette problématique.

Au nombre des cibles, on peut citer particulièrement les commutateurs et les routeurs, ainsi que tout élément d'infrastructure mais aussi principalement les utilisateurs et leurs services sur le réseau.

Les protocoles de résolution d'adresse IP comme ARP et ND sont des vecteur favoris et très vulnérables.

Pour empêcher des accès non-autorisés sur base des adresses L2 de bas niveau comme des adresses MAC, la fonctionnalité Cisco `port-security mac-address sticky` au menu de la certification CCNA est une mesure intéressante, mais elle est aisée à dépasser alors que sa gestion reste une contrainte.

Si la menace sur ces protocles ARP et ND est prise au sérieux, on s'orientera plus volontiers vers des solutions comme DAI (Deep ARP Inspection) ou IPv6 First Hop Security (notamment avec *RA Guard*).

Mais il y a tellement de services à disposition sur le réseau et ils sont si crédules qu'il convient de rester attentif aux menaces sur les protocoles d'infrastructure comme DHCP, DNS, NTP, SNMP ou encore les protocoles de routage dynamique (EIGRP, OSPF) ou de redondance de passerelle (HSRP, VRRP), mais les protocoles d'accès distant aux consoles (SSH et ancêtres comme Telnet ou Rlogin).

Sur les commutateurs (Cisco), on trouvera une série de protocoles L2 propriétaires ou IEEE 802.1 tels que 802.1.q, 802.1D, CDP, VTP, DTP, PaGP, LACP, etc., la plupart du temps activés par défaut et qui constituent autant de vulnérabilités intrinsèques à une configuration par défaut. Parmi beaucoup d'autres possibilités, activer `bpduguard` sur les ports Access et désactiver tout ce qui est inutile : CDP, VTP, DTP, les ports orphelins, etc., sont recommandées. Selon les conseils de Cisco, on évitera à tout prix d'utiliser le VLAN 1.

2.4. IEEE 802.1X / EAP / Radius

Enfin si les moyens de l'organisation le permettent et sa la volonté y est, on mettra en oeuvre une solution qui authentifie les utilisateurs avant de leur donner un accès (filaire ou non) de couche (L2) au réseau avec 8021.X/EAP/RADIUS. Si le choix de l'organisation s'oriente vers des solutions qui intègrent la gestion du réseau filaire et sans-fil de manière transparente, celle-ci est certainement prête pour un tel type de déploiement par l'obligation du support du protocole de sécurité de réseau sans-fil de type "WPA/WPA2 Enterprise" respectant la norme IEEE 802.11i intégrant IEEE 8021.X/EAP/RADIUS.

- PacketFence
- Microsoft NAP
- Cisco NAC
- HP, Aruba, …

2.5. Contre-mesures

- Sur les commutateurs : du filtrage (port-security, vACLs), de la vérification protocolaire (bpduguard, dai, ipv6 fhs, dhcp snooping), et de bonnes pratiques de configuration et de gestion.
- Dans l'infrastructure : de l'IDS/IPS généraliste (snort, surricata) ou spécialisé (arp-watch, ndpmon, packet-fence). Filtrage NTP et SNMP, Authentification NTP, authentification et chiffrement SNMP, authentification OSPF et EIGRP, authentification VRRP/HSRP.
- Sur les hôtes : au minimum des solutions de chiffrement TLS : HTTPS/HSTS, VPN TLS, IMAPS, SSH, … et un must avec une solution IDS/IPS/AV intégrée au périphérique terminal de type "End-Point Security" ; bannir les protocoles qui passent en clair (HTTP, SMTP, POP3).
- Sur les port d'accès des utilisateurs finaux : IEEE 8021.X/EAP/RADIUS, IEEE 802.11i, des communications VPN dans les réseaux tiers ou non-sécurisés.

- Une serveillance (*monitoring*) des événements avec de la journalisation (*logging*) et des alertes.

Deuxième partie Gestion d'infrastructure

Dans cette partie intitulé "Gestion d'infrastructure", on évoquera des pratiques de gestion comme la configuration des mots de passes, des accès distantes (Telnet, SSH) et locales, le transfert de fichiers (TFTP, FTP, SCP) et la vérification de fichiers (MD5).

On parlera ensuite de différents protocoles que les utilisateurs finaux ignorent car ils ne les utilisent pas directement. Mais ces protocoles de contrôle sont utiles voire indispensables à la gestion et à la surveillance du réseau. Aussi on conseillera de les faire fonctionner dans des canaux (des VLANs) dédiés à la gestion de l'infrastructure avec des politiques d'accès fines.

Parmi ces protocoles, on citera les protocoles de couche 2 (L2) tels que CDP (propriétaire Cisco) et LLDP (IEEE 802.1ab). On citera aussi SYSLOG (basé UDP) qui permet de collecter des messages venant des commutateurs, des routeurs ou des serveurs. Mais à quoi bon collecter des logs s'ils ne sont pas à la bonne heure ? NTP (basé UDP) permet de synchroniser les horloges à travers le réseau.

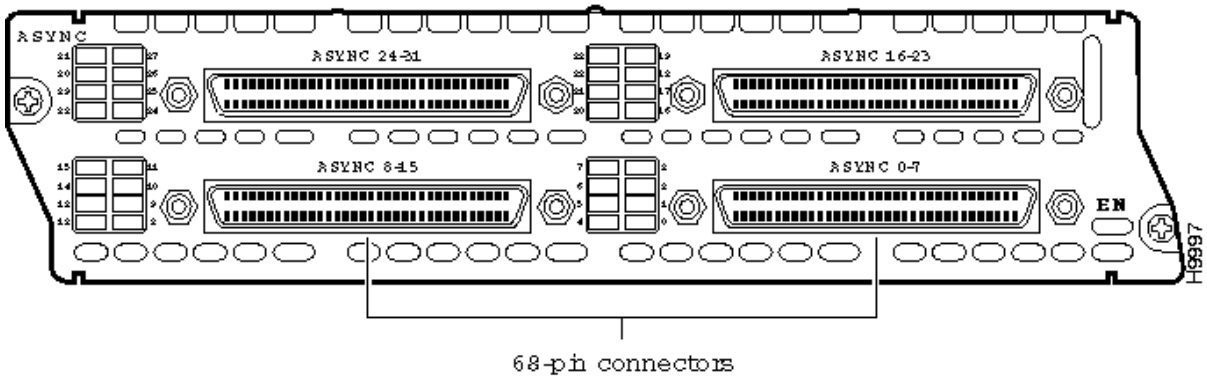
2. Configuration et gestion des consoles Cisco IOS

Ce chapitre traite du sujet de la configuration et de la gestion des consoles locales et distantes (Telnet et SSH) des périphériques Cisco ainsi que de leur sécurisation.

1. Consoles physiques et distantes

1.1. Lignes

- lignes physiques : connexion série asynchrone (port `con0`), connexion série avec contrôle de flux (port `aux0` sur les routeurs et absent des commutateurs), ou encore une carte serveur de console Cisco “Network Module” (NM-16A ou NM-32A) à insérer dans un routeur de concentration et à utiliser avec un câble octal de type “CAB-OCTAL-ASYNC=” ou “CAB-OCTAL-MODEM=”.
- lignes distantes : protocoles TCP/IP qui offrent un service de console comme SSH mais aussi bien d’autres antécédents que l’on ne recommande plus d’utiliser aujourd’hui (Telnet, Rlogin, Rsh, etc.).



Understanding 16- and 32-Port Async Network Modules

Source de l’image : Understanding 16- and 32-Port Async Network Modules.

La commande `show line` permet de visualiser les consoles disponibles sur le périphérique Cisco. On trouve trois types de “lignes” :

- **`CTY`** : correspond au port `con 0`.
- **`AUX`** : correspond au port `aux 0`
- **`VTY`** : correspond à toutes les connexions distantes qui ont ouvert un port virtuel de `vty 0` à `vty 4`.

Dans cet exemple, on trouve une connexion sur le terminal `0` (connexion console physique) et une autre sur le terminal `2` (connexion Telnet).

```
#show line
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0 CTY              -    -      -    -    -      0       1     0/0       -
     1 AUX   9600/9600  -    -      -    -    -      0       0     0/0       -
*    2 VTY              -    -      -    -    -      2       0     0/0       -
     3 VTY              -    -      -    -    -      0       0     0/0       -
     4 VTY              -    -      -    -    -      0       0     0/0       -
     5 VTY              -    -      -    -    -      0       0     0/0       -
     6 VTY              -    -      -    -    -      0       0     0/0       -
```

Une configuration par défaut donne deux consoles physiques et cinq terminaux virtuels de `vty 0` à `vty 4`.

```
#show run | begin line
line con 0
line aux 0
line vty 0 4
 login
 transport input none
!
end
```

Vérification de la configuration du terminal courant.

Dans une session `con 0`

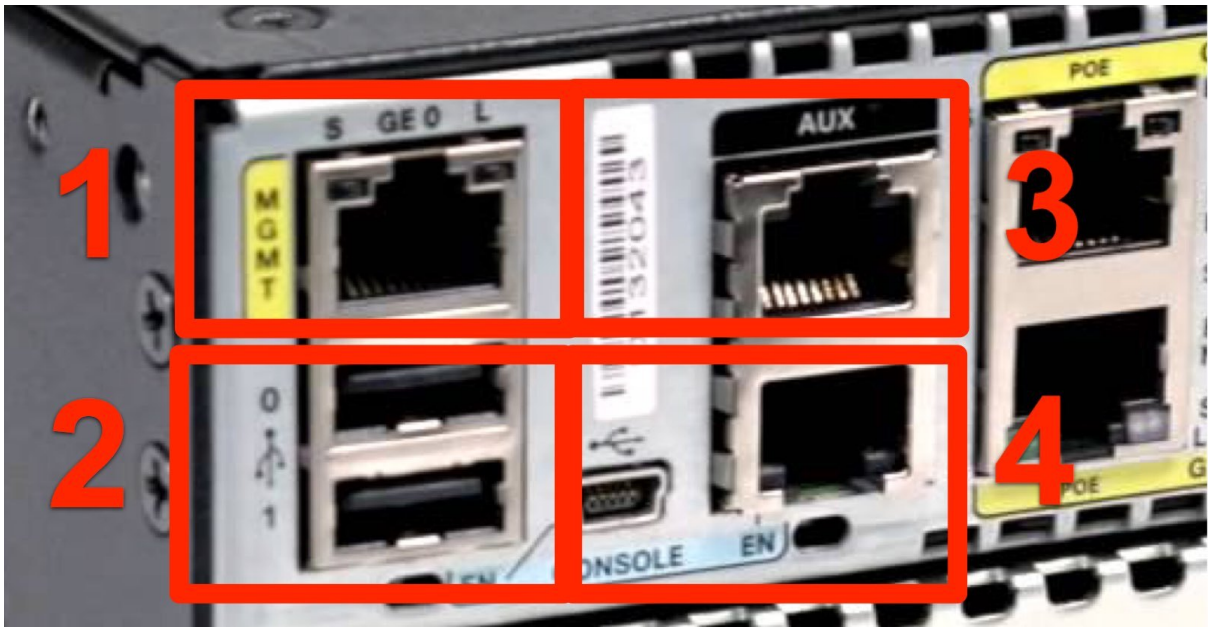
```
SW0#show terminal
Line 0, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Status: PSI Enabled, Ready, Active, Automore On
Capabilities: none
Modem state: Ready
Group codes:    0
Modem hardware state: CTS* noDSR  DTR RTS
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               00:10:00        never                       none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
Time since activation: 00:13:11
Editing is enabled.
History is enabled, history size is 20.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed input transports are none.
Allowed output transports are lat pad telnet rlogin nasi ssh.
Preferred transport is lat.
Shell: disabled
Shell trace: off
No output characters are padded
No special data dispatching characters
```

Avec une connexion SSH distante.

```
SW0#show terminal
Line 2, Location: "", Type: "vt100"
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: PSI Enabled, Ready, Active, No Exit Banner, Automore On
  Notify Process
Capabilities: none
Modem state: Ready
Group codes:    0
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               00:10:00        never                        none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
Time since activation: 00:00:13
Editing is enabled.
History is enabled, history size is 20.
```

1.2. Consoles locales

On trouve deux ports “console”, `con0` et `aux0` sur les routeurs la plupart du temps sur la façade arrière à proximité des interfaces de communication. Le second port auxiliaire totalement indépendant du premier gère le contrôle de flux et se connecte à l’interface DB-25 d’un modem analogique.



Façade d’un routeur Cisco ISR 4451-X

- (1) : Interface `G0` de gestion (management)
- (2) : Ports USB type B pour du stockage

- (3) : Ports USB type A et RJ-45 `con 0` comme console locale
- (4) : Port auxiliaire `aux 0` pour connecter un modem ananlogique.

image !!!!

On trouve un seul port `con0` sur les commutateurs Cisco, à l'arrière du périphérique. à l'opposé de l'alimentation électrique.

image !!!!

Configuration en ROM Monitor Mode … –> référence

logging synchronous

1.3. Authentification nulle

…

1.4. Authentification par mot de passe

Cette méthode est ici pour mémoire et ne doit plus être utilisée

1.5. Authentification par nom d'utilisateur

…

1.6. Configuration d'un service telnet sous Cisco IOS

…

1.7. Connexion à un routeur en Telnet

2. Accès distant Secure Shell (SSH)

Secure Shell (SSH) est un protocole qui permet de sécuriser les communications de données entre les ordinateurs connectés au réseau en assurant la confidentialité, l'intégrité, l'authentification et l'autorisation des données dans des tunnels chiffrés. Il utilise TCP habituellement sur le port 22, mais il peut en utiliser d'autres simultanément. Il est fondé sur le protocole TLS. On utilise aujourd'hui la version SSH-2. La version SSH-1 est à éviter. Il supporte les authentifications centralisées (PAM), locale avec mot de passe ou sans (par le biais d'échange de clés).

2.1. Cas d'usage du protocole SSH

Les sous-protocoles SCP et SFTP offrent des services de transfert de fichiers.

On peut l'utiliser comme console distante à la manière de Telnet, RSH ou Rlogin.

On peut y transférer des ports et utiliser le service comme proxy ou comme solution VPN.

On peut transférer des sessions X graphiques dans un tunnel SSH.

Il s'intègre à des logiciels comme `ansible`, `systemd`, `x2go`, …

2.2. Sécurité de SSH

En termes de cible d'attaque, le port est très sollicité par les robots qui "scannent" les réseaux publics en quête de configurations faibles, nulles, négligées ou exploitables. Il peut arriver qu'un port SSH exposé publiquement soit l'objet de tentatives de "Déni de Service" (DoS) ou de connexions "Brute Force" qui rendent le service inaccessible.

Il est conseillé d'auditer, voire de filter les accès au service avec un logiciel comme `fail2ban`, des sondes IPS/IDS `snort`, `surricate` ou encore d'autres. Un pot de miel tel que `cowrie` peut être un outil à manipuler avec précaution. Des projets comme Modern Honey Network (MHN) peuvent faciliter le déploiement de telles sondes.

Les authentifications par clé sans mot de passe, les restrictions dans la configuration du serveur SSH ainsi qu'une politique d'accès et de mot de passes forts sont recommandés.

2.3. Configuration d'un serveur SSH en Cisco IOS

ref : https ://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-mt/sec-usr-ssh-15-mt-book/-sec-usr-ssh-sec-shell.html

- FQDN
- crypto key gen rsa mod (crypto key zeroize rsa)
- activer la version 2
- Configurer un utilisateur
- Configurer les lignes VTY
- ip ssh {timeout seconds | authentication-retries integer}
- show ip ssh
- show ssh
- debug ip ssh

```
ip ssh timeout 60
ip ssh authentication-retries 2
```

```
hostname R1
ip domain-name entrepise.lan
enable secret <secret>
username <user> privilege 15 algorithm-type sha256 secret <secret>
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
```

2.4. Connexion en SSH à partir d'un client Cisco IOS

...

| SSH command parameters | Description | | — | — | | `-v` | specifies whether we are going to use version 1 or version 2 | | `-c {3des | aes128-cbc | aes192-cbc j aes256-cbc}` | specifies the encryption you are going to use when communicating with the router. This value is optional ; if you choose not to use it, the routers will negotiate the

encryption algorithm to use automatically | | `-l username` | specifies the username to use when logging in to the remote router `-m {hmac-md5 | hmac-md5-96 | hmac-sha1 | hmac-sha1-96}` | specifies the type of hashing algorithm to use when sending your password. It is optional and if you do not use it, the routers will negotiate what type of hashing to use. |

For example the command “ssh -v 2 -l admin 10.1.1.1” means “use SSH version 2 to connect to a router at 10.1.1.1 with username “admin”.

2.5. Logiciels SSH pour Windows

- Utilitaire Putty : http ://www.chiark.greenend.org.uk/∼sgtatham/putty/download.html
- Utilitaire CyberDuck : https ://cyberduck.io/
- Utilitaire WinSCP : https ://winscp.net/eng/docs/lang :fr
- Serveur X Xming : https ://sourceforge.net/projects/xming/

Windows 10 intègre nativement les logiciels OpenSSH.

2.6. Reverse SSH en Cisco IOS

Reverse SSH : https ://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-mt/sec-usr-ssh-15-mt-book/sec-rev-ssh-enhanmt.html

3. Sécurisation des accès de gestion

3.1. Timeout sur les consoles

```
Router1(config-line)#exec-timeout 240 0
absolute-timeout 5
logout-warning 30
```

3.2. Bannières Cisco IOS

```
banner exec ^C
**********************
* Banner exec        *
**********************^C
banner incoming ^C
**********************
* Banner incoming    *
**********************^C
banner login ^C
**********************
* Banner login       *
**********************^C
banner motd ^C
**********************
* Banner motd        *
**********************^C
```

Seulement le protocole activé (????), les options de la commande `banner`

Option de la commande banner	Telnet	SSH v1 seulement	SSH v1 et v2	SSH v2 seulement
`banner login`	**S'affiche avant l'authentification.**	*Ne s'affiche pas.*	S'affiche avant l'authentification.	S'affiche avant l'authentification.
`banner motd`	*S'affiche avant l'authentification.*	**S'affiche après l'authentification.**	S'affiche après l'authentification.	S'affiche après l'authentification.
`banner exec`	**S'affiche après l'authentification.**	S'affiche après l'authentification.	S'affiche après l'authentification.	S'affiche après l'authentification.

Source : http ://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html#banners

On peut utiliser différents "Tokens" qui s'utilisent comme des variables d'environnement dans les bannières.

Token | Description — | — `$(hostname)` | Nom du périphérique `$(domain)` | Nom de domaine du périphérique `$(line)` | Numéro de ligne de terminal `$(line-desc)` | Description de la ligne de terminal

```
Router1(config-line)#no motd-banner
Router1(config-line)#no exec-banner
```

3.3. Filtrage VTY

```
(config)#ip access-list extended VTY
(config-ext-nacl)#permit ip host 172.16.0.1 any
(config-ext-nacl)#permit ip 192.168.56.0 0.0.0.255 any
(config-ext-nacl)#exit


(config)#line vty 0 4
(config-line)#ip access-class VTY in
```

3.4. Authentification SSH par clé RSA

Le client s'authentifie avec sa clé privée. Le serveur authentifie le client avec la clé publique (du client installée sur le serveur).

Sur le client :

```
ssh-keygen -b 1024
cat .ssh/id_rsa.pub
```

Sur le matériel cisco :

```
ip ssh pubkey-chain
 username root
 key-string
<copie de id_rsa.pub>
```

et plusieurs fois la commande exit.

3.5. Gestion des connexions

Voir les utilisateurs connectés :

```
SW0#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                idle                 00:00:00
   2 vty 0     root       idle                 00:00:14 192.168.1.254

  Interface    User               Mode         Idle     Peer Address
```

3.6. Désactivation des consoles

```
To completely disable access via the router’s AUX port, use the following set of commands:

Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#line aux 0
Router1(config-line)#transport input none
Router1(config-line)#no exec
Router1(config-line)#exec-timeout 0 1
Router1(config-line)#no password
Router1(config-line)#exit
Router1(config)#end
Router1#
You can disable access to the router through the VTY lines as follows:

Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#access-list 98 deny any log
Router1(config)#line vty 0 4
Router1(config-line)#transport input none
Router1(config-line)#exec-timeout 0 1
Router1(config-line)#no exec
Router1(config-line)#access-class 98 in
Router1(config-line)#exit
Router1(config)#end
Router1#
```

3.7. Logguer des accès

Agir sur l’ACL vty `deny ip any any log` et `deny ipv6 any any log`.

4. Annexe pour mémoire

Niveau de privilège

... Ref CCNA Security

Accès au CLI “Role Based” (view)

... Ref CCNA Security

Authentifications AAA / Radius

... Ref CCNA Security

Troisième partie Automation et Programmabilité

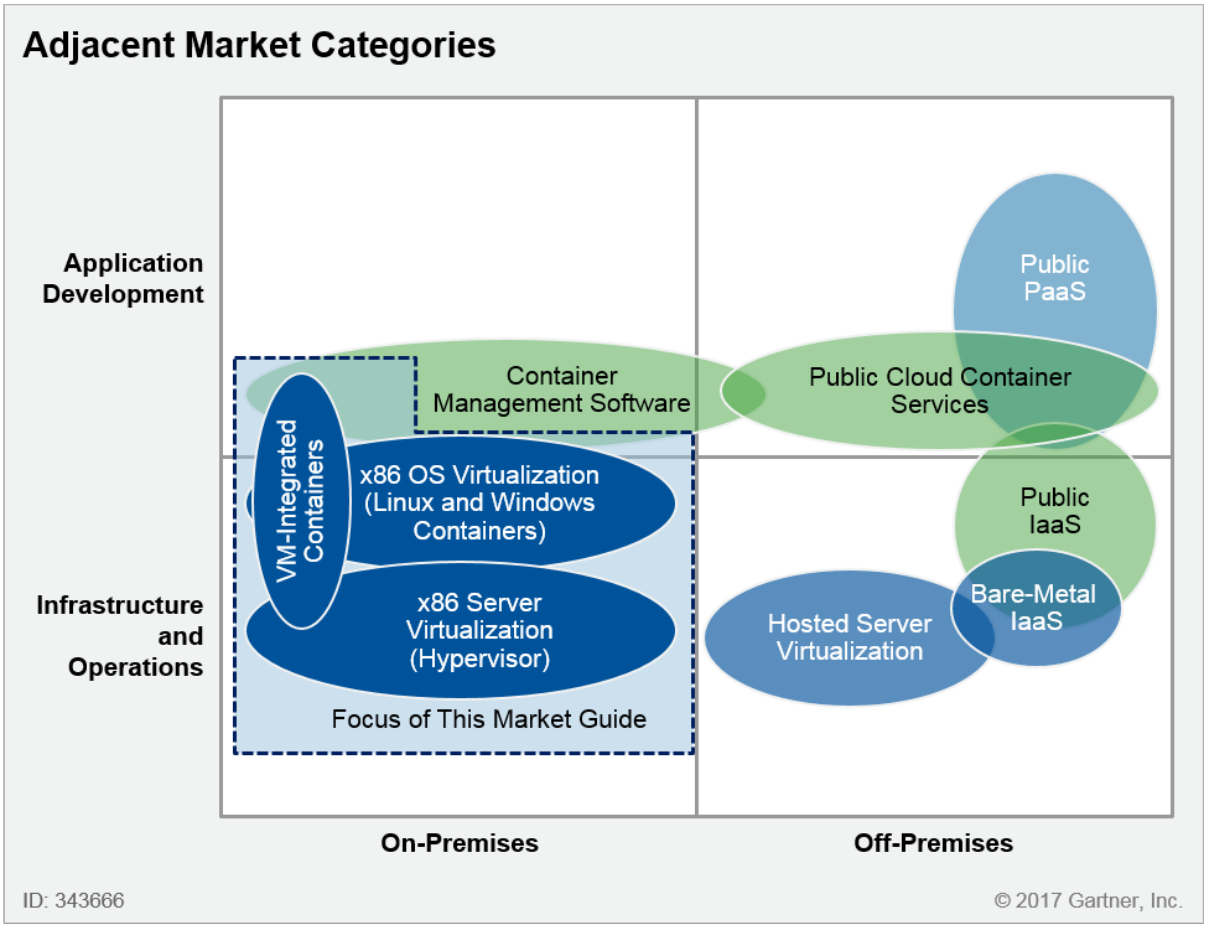
Cette partie sur l'automation et la programmabilité du réseau est en cours de révision. Il portera sur les architectures contrôlées de type SDN, sur le concept d'Intent Based Network, d'automation et d'outils d'automation. Enfin, on terminera sur le protocole HTTP, les actions CRUD, la manipulation d'APIs HTTP REST et le traitement des sorties en format de présentation JSON.

3. De la virtualisation au nuage

La virtualisation des ordinateurs est une idée aussi vieille[1] que celle de l'ordinateur.[2] Mais depuis la seconde décade du XXIème siècle, la virtualisation est devenue une forme commune et maîtrisée pour exécuter des charges informatiques. La virtualisation est un élément constitutif et essentiel de nos infrastructures informatiques contemporaines ; elle est une "brique de base" pour tout marché proposant les architectures qui supportent cette charge, dans nos entreprises mais aussi dans le nuage rendant ce modèle possible, parmi d'autres facteurs.

Pour le commun des mortels, la virtualisation peut sembler étrange, voire difficile à comprendre, car il s'agit d'abstraire des composants informatiques matériels et logiciels principalement du côté des serveurs dont les clients ignorent tout du fonctionnement et des enjeux en terme de gestion, de maintenance et d'optimisation.

Mais la virtualisation fait partie d'un paradigme informatique plus large reprenant un phénomène de dématérialisation des services. A titre d'exemple, la virtualisation est un élément essentiel voire constitutif de l'informatique en nuage (*Cloud Computing*) dans lequel la technologie TCP/IP et l'accès au réseau devient critique. La charge est alors exécutée à distance à partir de requêtes de clients de plus en plus légers et hétérogènes à destination de services virtualisés dans le nuage.



Gartner abandonne le Magic Quadrant x86 Server Virtualization Infrastructure (16 mars 2017).

On trouvera aujourd'hui deux types de virtualisation : la virtualisation matérielle (dématérialisant l'infrastructure) et la virtualisation logicielle (dématérialisant les applications). On trouvera aussi deux types de déploiement de

1. Magic Quadrant for Network Firewalls Published 17 September 2019 - ID G00375686
2. Elle lui est probablement intrinsèque tel que l'évoque le modèle abstraut de la machine de Turing.

la virtualisation : en local (*on-premise*), dans l'entreprise, et dans le nuage. Gartner[3] nous suggère d'élargir notre vision de la virtualisation des plate-formes x86 d'entreprise de manière bimodale en direction du nuage et de la conteneurisation.

1. Virtualisation

1.2. Objectif de la virtualisation

L'objectif principal de la virtualisation est l'usage efficient de ressources de calcul partagées entre plusieurs entités virtuelles : mémoire, processeur, réseau, stockage sont partagés efficacement dans la perspective d'économies d'échelle. Cet objectif correspond aux principes actuels de gestion des systèmes d'information.

On pourrait résumer ce principe de deux manières : "faire autant avec moins" ou "faire plus avec autant". Il peut s'agir de gains d'énergie, de place, de maintenance, de gestion, de comptabilité, de robustesse, d'évolutivité, de conception, etc. Bref il s'agit de dimensionner de manière optimale son infrastructure et de répondre aux besoins de l'entreprise de manière souple. Le marché et ses acteurs s'engouffre alors dans cette logique.

Aussi, la virtualisation des serveurs permet une bien plus grande modularité dans la répartition des charges et la reconfiguration des serveurs en cas d'évolution ou de défaillance momentanée (plan de secours, etc.).

1.3. Définition formelle

De manière formelle, la virtualisation consiste en la séparation logique entre, d'une part, les ressources fournissant un service et, d'autre part, le service lui-même.

Mais le terme "virtualisation" en informatique est à mettre en relation avec différentes techniques et en différents contextes, parmi beaucoup d'autres citons les concepts suivants :

- Dématérialisation
- Emulation
- Virtualisation matérielle
- Virtualisation logicielle
- Virtualisation d'infrastructure

1.4. Dématérialisation

Par l'intermédiaire de technologies diverses, il est alors possible de dématérialiser les plateformes matérielles, les infrastructures et les services. On peut dématérialiser les serveurs, les bureaux (desktop) informatiques, les emplacements de stockage, l'accès à différents services.

1.5. Emulation matérielle

La virtualisation matérielle n'est pas la même chose que l'émulation matérielle. Avec l'émulation matérielle, une pièce de matériel en imite une autre, tandis qu'avec la virtualisation matérielle, un hyperviseur (une pièce de logiciel) imite une pièce de matériel informatique particulière ou l'ordinateur entier. En outre, un hyperviseur n'est pas la même chose qu'un émulateur ; ce sont tous deux des programmes informatiques qui imitent le matériel, mais leur domaine d'utilisation diffère légèrement.[4]

L'émulation et la virtualisation sont liées, mais pas identiques. L'émulation consiste à utiliser un logiciel, un émulateur, pour fournir un environnement d'exécution ou une architecture différente. Par exemple, vous pouvez

3. The future of server virtualization, source de l'image : Gartner abandonne le Magic Quadrant x86 Server Virtualization Infrastructure (16 mars 2017).
4. Source : Hypervisor.

faire fonctionner un émulateur Android sur une machine Windows. L'ordinateur Windows (Intel x86) n'a pas le même processeur qu'un appareil Android (ARM), de sorte que l'émulateur exécute en fait l'application Android par le biais d'un logiciel.[5]

2. Virtualisation des architectures x86

La **virtualisation des ordinateurs x86** consiste à séparer les ressources matérielles (en CPU/RAM, réseau et stockage) des services rendus par ces ressources, à savoir des applications informatiques. Concrètement sur un même ordinateur physique, on pourra créer plusieurs machines virtuelles (VM) distinctes dédiées à des applications spécifiques. En bref, la virtualisation telle qu'on l'entend communément est la mutualisation des systèmes d'exploitation ou d'applications sur un seul ou plusieurs serveurs physiques.

A titre d'exemple, dans le milieu des années 2000, on assiste à ce qu'on appelle la consolidation des centres de données (salle serveurs, *datacenters*). Elle avait déjà commencé avec la virtualisation du réseau (VLAN) et du stockage (NAS/SAN). La société VMWare très active sur ce segment de marché proposa des produits et des services complets de virtualisation de serveurs à architecture x86. Sur ce segment de marché des concurrents tels que Microsoft ou Citrix menèrent un guerre stratégique. Leur avantage consiste à fournir un environnement de gestion intégré.

2.1. Virtualisation

La virtualisation consiste plutôt à créer des barrières virtuelles entre plusieurs environnements virtuels fonctionnant dans le même environnement physique. La grande différence est que l'environnement virtualisé est la même architecture. Une application virtualisée peut fournir des appareils virtualisés qui sont ensuite traduits en appareils physiques et l'hôte de virtualisation a le contrôle sur la machine virtuelle qui a accès à chaque appareil ou partie d'appareil. L'exécution réelle est le plus souvent encore exécutée en mode natif, et non par logiciel. Par conséquent, les performances de la virtualisation sont généralement bien meilleures que celles de l'émulation.[6]

2.2. Hyperviseur

Le terme *hyperviseur* est une variante de *superviseur*, un terme traditionnel pour désigner le noyau d'un système d'exploitation : l'hyperviseur est le superviseur du superviseur.

Un hyperviseur (ou moniteur de machine virtuelle, VMM) est un logiciel, un micrologiciel ou un matériel informatique qui crée et fait fonctionner des machines virtuelles. Un ordinateur sur lequel un hyperviseur fait tourner une ou plusieurs machines virtuelles est appelé machine hôte, et chaque machine virtuelle est appelée machine invitée.[7]

2.3. Machine virtuelle

La virtualisation matérielle consiste à présenter les ressources matérielles (CPU/RAM, stockage, réseau entrées/-sorties) d'un hôte physique sous forme logicielle et de les partager auprès d'une machine virtuelle. Une machine virtuelle se comporte en tout point comme un véritable ordinateur de telle sorte que sa gestion relève des même principes sauf qu'il ne s'agit plus de gérer des objets physiques mais une réalité technique tel qu'un fichier.

Pour l'essentiel, une machine virtuelle (VM, Virtual Machine) est composée de fichiers qui sont interprétés et lus par l'hyperviseur de l'hôte physique qui partage ses ressources CPU/RAM, stockage et réseau. On trouvera au minimum deux fichiers : celui qui définit la machine virtuelle et celui qui représente un disque qui lui est attaché (une mémoire de masse).

Un fichier de définition formelle de la VM comme une sorte de description d'une carte mère physique qui détermine le type de processeur (CPU), la quantité de mémoire vive (RAM), les différents bus d'entrée et de sortie (I/O) ainsi que le chemin qui indique l'emplacement des disques virtuels. Ce fichier est en général directement lisible en format texte

5. Source : Full emulation vs. full virtualization, Stack Overflow
6. Source : Full emulation vs. full virtualization, Stack Overflow
7. Source : Hypervisor

de type “ini” ou en format XML. Les caractéristiques de la VM peuvent être immédiatement données en argument à l’hyperviseur qui l’exécute.

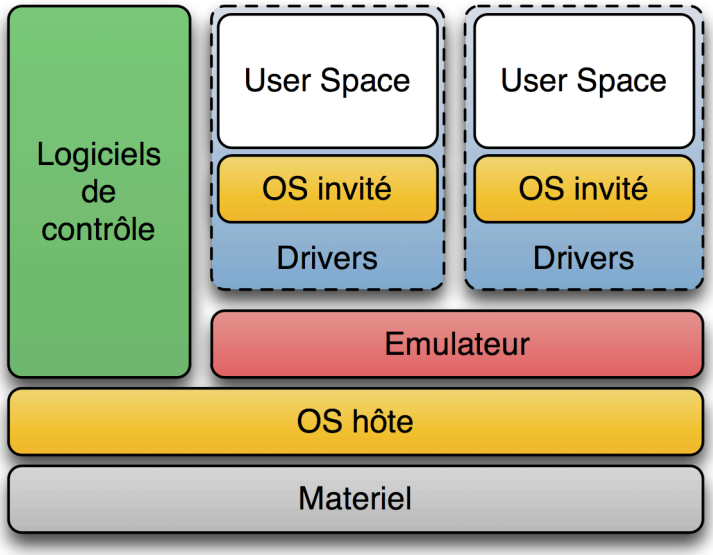
Des fichiers binaires qui représentent les disques des VMs et qui peuvent être dupliqués et manipulés sans limite. On parle alors de l’art de fabriquer des images. Les formats de disques virtuels les plus connus sont `vmdk`, `raw` ou encore `qcow2`. Mais cette mémoire de masse pourrait être un LUN i-SCSI directement connecté à la VM.

On trouvera d’autres fichiers temporaires, des journaux qui ne sont pas nécessairement indispensables à son fonctionnement.

Il existe également un concept distinct de machine virtuelle, comme celles qui exécutent du code Java, .NET ou Flash. Elles peuvent varier d’une implémentation à l’autre et peuvent inclure des aspects d’émulation ou de virtualisation, ou les deux. Par exemple, la JVM fournit un mécanisme permettant d’exécuter des codes d’octets Java. Toutefois, les spécifications de la JVM ne stipulent pas que les codes d’octets doivent être exécutés par un logiciel ou qu’ils doivent être compilés en code natif. Chaque JVM peut faire ce qu’elle veut et, en fait, la plupart des JVM font une combinaison des deux en utilisant l’émulation lorsque c’est approprié et en utilisant un JIT lorsque c’est approprié (le Hotspot JIT est le nom donné à la JVM de Sun/Oracle).[8]

2.4. Hyperviseur de type 2

“Un hyperviseur de type 2 est un logiciel (généralement assez lourd) qui tourne sur l’OS hôte. Ce logiciel permet de lancer un ou plusieurs OS invités. La machine virtualise ou/et émule le matériel pour les OS invités, ces derniers croient dialoguer directement avec ledit matériel.”



Hyperviseur de type 2

“Cette solution est très comparable à un émulateur, et parfois même confondue. Cependant l’unité centrale de calcul, c’est-à-dire le microprocesseur, la mémoire de travail (ram) ainsi que la mémoire de stockage (via un fichier) sont directement accessibles aux machines virtuelles, alors que sur un émulateur l’unité centrale est simulée, les performances en sont donc considérablement réduites par rapport à la virtualisation.”

“Cette solution isole bien les OS invités, mais elle a un coût en performance. Ce coût peut être très élevé si le processeur doit être émulé, comme cela est le cas dans l’émulation. En échange cette solution permet de faire cohabiter plusieurs OS hétérogènes sur une même machine grâce à une isolation complète. Les échanges entre les machines se font via les canaux standards de communication entre systèmes d’exploitation (TCP/IP et autres protocoles réseau), un tampon d’échange permet d’émuler des cartes réseaux virtuelles sur une seule carte réseau réelle.”[9]

8. Source : Full emulation vs. full virtualization, Stack Overflow
9. Source du texte et de l’image : Virtualisation et Hyperviseur de type 2.

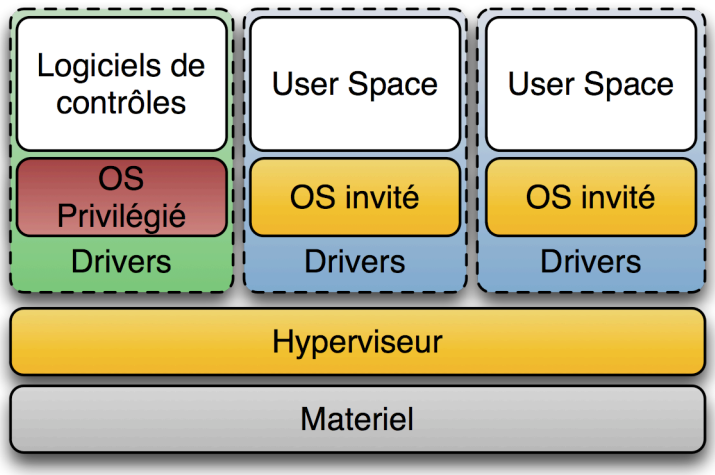
Exemples :

- Parallels Desktop
- Oracle VM VirtualBox
- VMware Fusion, VMware Player, VMware Server, VMware Workstation

2.5. Hyperviseur de type 1

"Un hyperviseur de type 1 est comme un noyau système très léger et optimisé pour gérer les accès des noyaux d'OS invités à l'architecture matérielle sous-jacente. Si les OS invités fonctionnent en ayant conscience d'être virtualisés et sont optimisés pour ce fait, on parle alors de paravirtualisation."

"Actuellement l'hyperviseur est la méthode de virtualisation d'infrastructure la plus performante mais elle a pour inconvénient d'être contraignante et onéreuse, bien que permettant plus de flexibilité dans le cas de la virtualisation d'un centre de données."[10]



Hyperviseur de type 1

Exemples :

- Xen (libre)
- VMware ESXi
- Microsoft Hyper-V Server
- Parallels Server Bare Metal
- KVM (libre)

2.6. Virtualisation totale (Full virtualization)

Dans la plupart des cas, il s'agit de la technique de virtualisation utilisées par les hyperviseurs de type 2. Dans ce cas le matériel est suffisamment émulé pour permettre à un système d'exploitation de fonctionner sans modification.[11]

10. Source du texte et de l'image : Virtualisation et Hyperviseur de type 1.
11. Source : Full virtualization

Cette approchée a été implémentée en 1966 avec l' IBM CP-40 et CP-67, prédécesseurs de la familleVM. Les exemples en dehors du secteur des mainframes : Parallels Workstation, Parallels Desktop for Mac, VirtualBox, Virtual Iron, Oracle VM, Virtual PC, Virtual Server, Hyper-V, VMware Workstation, VMware Server (GSX Server), KVM, QEMU, Adeos, Mac-on-Linux, Win4BSD, Win4Lin Pro, et Egenera vBlade technology.

2.7. Virtualisation Hardware-Assisted

Le support de la virtualisation totale peut être intégré au processeur ou assisté par celui-ci, le matériel se chargeant, par exemple, de virtualiser les accès mémoire ou de protéger le processeur physique des accès les plus bas niveau. Cela permet de simplifier la virtualisation logicielle et de réduire la dégradation de performances.[12]

Des exemples de virtualisation matérielle :

- Hyperviseur IBM Power & Micro-partitionnement AIX
- Mainframes : VM/CMS
- Sun LDOM (hyperviseur pour la gestion de “logical domains”)
- Sun E10k/E15k
- HP Superdome
- AMD-V (Assistance à la virtualisation de AMD, anciennement Pacifica)
- Intel VT (Assistance à la virtualisation de Intel, anciennement Vanderpool)

Cette technique de virtualisation est aussi connue sous le nom de virtualisation accélérée ; Xen appelle cette technique **Hardware Virtual Machine (HVM)**.

Des solutions bien connues qui implémentent les instructions VT-x et AMD-V sur architectures x86 sont par exemple VMware Workstation ou VMWare ESX , Xen 3.x+ (et ses dérivatifs), Linux KVM et Microsoft Hyper-V.

2.8. Paravirtualisation

La paravirtualisation est une réponse à la difficulté de virtualiser une bonne partie de l’ensemble des instructions des processeurs x86. Cette approche connait également des antécédents technologiques.

La paravirtualisation est une technique de virtualisation qui présente à une machine virtuelle une interface logicielle similaire à du matériel réel mais qui est optimisée pour ce type de fonctionnement. Cette approche s’oppose à l’émulation d’un périphérique matériel existant, qui peut s’avérer laborieuse et surtout plus lente.[13]

La paravirtualisation permet :

- aux moniteurs de machines virtuelles (VMM) d’être plus simples et
- aux machines virtuelles fonctionnant dessus d’atteindre un niveau de performance proche du matériel réel.

2.9. Transformation/portage du système d’exploitation invité

Cependant, les systèmes d’exploitation doivent explicitement être transformés afin de fonctionner sur des VMM paravirtualisées. Le portage des systèmes d’exploitation libres est généralement effectué, seulement il appartient aux fournisseurs de systèmes fermés de réaliser le portage eux-mêmes, ce qu’ils peuvent refuser de faire pour des raisons stratégiques.

12. Source : Hardware-assisted virtualization
13. Paravirtualisation

Le système modifié de la machine virtuelle est capable d'établir des hypercalls (appels hyperviseurs), soit une interface qui lui permet d'interagir plus directement et plus simplement avec le matériel. Des gains de performance sont alors constatés.

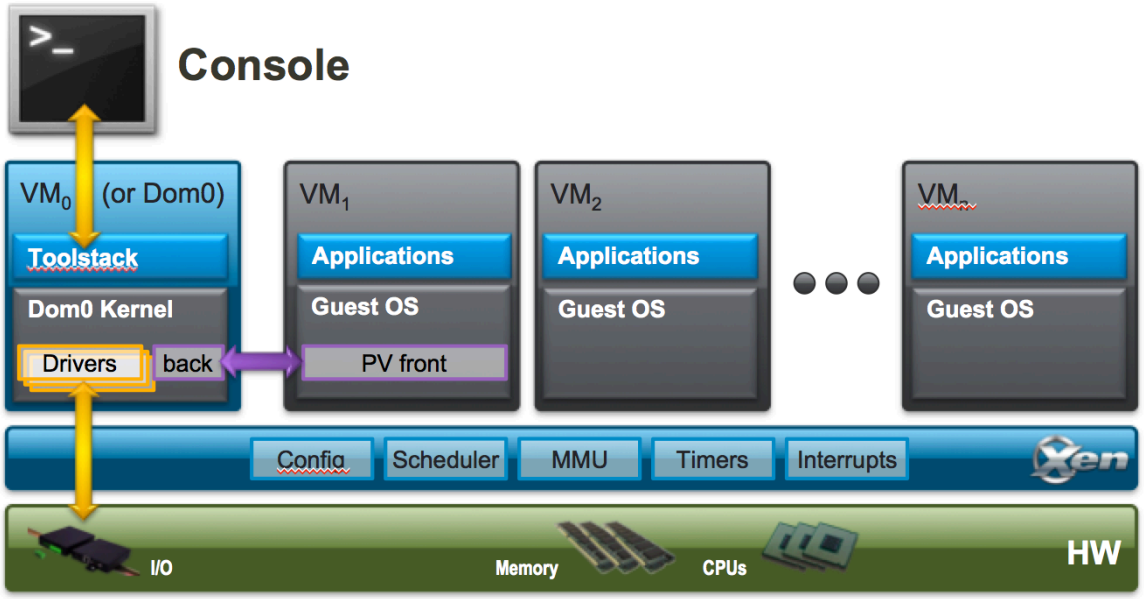
Exemples : IBM'sLPARs, Win4Lin 9x, Sun's Logical Domains, Xen et TRANGO

C'est sur base de cette approche de cette approche que le projet Xen se bat sur le marché de la virtualisation notamment par le canal commercial de la société Citrix Systems.

Suite à la prolifération de solutions de paravirtualisation sous Linux, chacune proposant une adaptation différente du noyau Linux, une solution commune est en cours de développement dans le noyau officiel : virtio. Elle voit ses débuts dans la version 2.6.24 et de nombreuses améliorations sont en cours dans la branche 2.6.25. Cette interface est déjà utilisée par KVM.

Les pilotes "virtio" sont similaires aux "vmware-tools" de VMWare ou "vb-tools" de VirtualBox.

Xen, supporté par Citrix et principal hyperviseur chez AWS, se différencie de par son architecture et son exploitation de la paravirtualisation.[14]



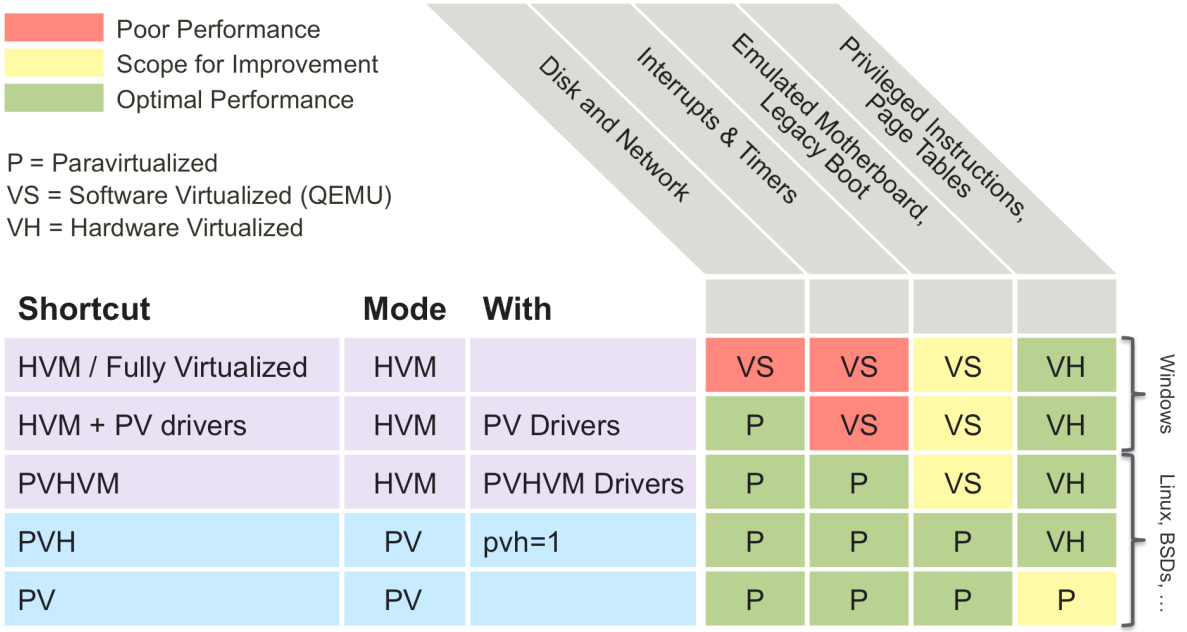
Architectture Xen

2.10. Synthèse des techniques de virtualisation de plateforme x86

Virtualisation Hardware	Paravirtualisation
OS invité non modifié	OS invité modifié (Linux/BSD)
La machine virtuelle se comporte comme une machine physique	La machine virtuelle connait son statut virtualisé
Peut faire fonctionner Windows	Ne peut faire fonctionner que des OS libres, mais aussi MS Windows (en PVHM)

La figure suivante montre la différence entre les virtualisations HVM (et ses variantes), PV et PVH avec Xen.[15]

14. Source de l'image : https ://wiki.xen.org/images/6/63/Xen_Arch_Diagram.png
15. Xen Project



La différence entre HVM (et ses variantes), PV et PVH

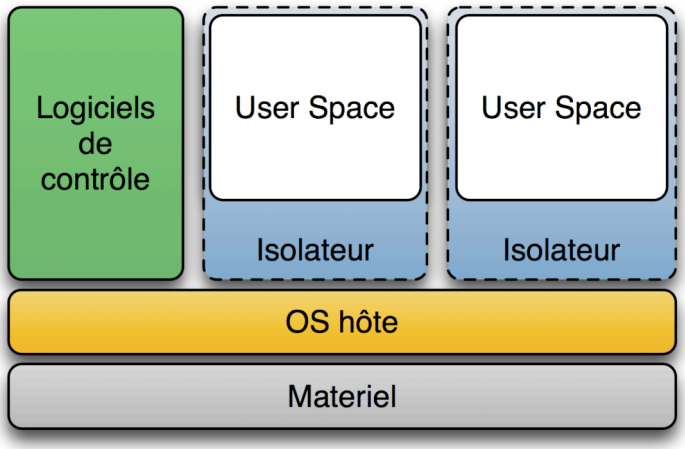
3. Virtualisation des applications

3.1. Isolateur

"Un isolateur est un logiciel permettant d'isoler l'exécution des applications dans ce que l'on appelle des contextes ou bien zones d'exécution. L'isolateur permet ainsi de faire tourner plusieurs fois la même application dans un mode multi-instance (plusieurs instances d'exécution) même si elle n'était pas conçue pour ça."

"Cette solution est très performante, du fait du peu de surcharge (temps passé par un système à ne rien faire d'autre que se gérer), mais les environnements virtualisés ne sont pas complètement isolés."

"La performance est donc au rendez-vous, cependant on ne peut pas vraiment parler de virtualisation de systèmes d'exploitation. Les isolateurs sont en fait composés de plusieurs éléments et peuvent prendre plusieurs formes."[16]



Isolateur

16. Source du texte et de l'image : Virtualisation et Isolateur

Quelques exemples de ce type de virtualisation par isolateur :

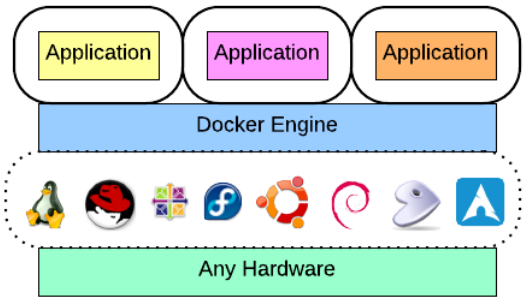
- Linux-VServer : isolation des processus en espace utilisateur ;
- chroot : isolation changement de racine ;
- BSD Jail : isolation en espace utilisateur ;
- OpenVZ : libre, partitionnement au niveau noyau sous Linux ;
- LXC : libre, usage des Cgroups du noyau Linux.
- Docker

3.2. Conteneur

> "*A container is a self contained execution environment that shares the kernel of the host system and which is (optionally) isolated from other containers in the system.*"[17]

Un container est un environnement d'exécution complet, autonome :

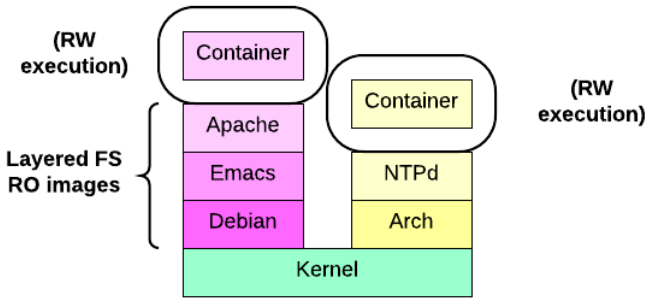
- qui partage le noyau du système hôte
- et qui est éventuellement isolé des autres processus du système.



Virtualisation par container

3.3. Registre d'images de conteneur

Les **containers** sont les exécutions en mode Lecture/écritures(RW) des images en lecture seule (RO) en tant qu'environnements virtuels.



Images et containers

17. https ://github.com/docker/libcontainer

Une **image** est un modèle statique d'un système de fichiers en mode Read-Only (RO). Il peut s'agir du rootfs Debian ou de n'importe quelle distribution. On travaille en général à partir d'une image de base.

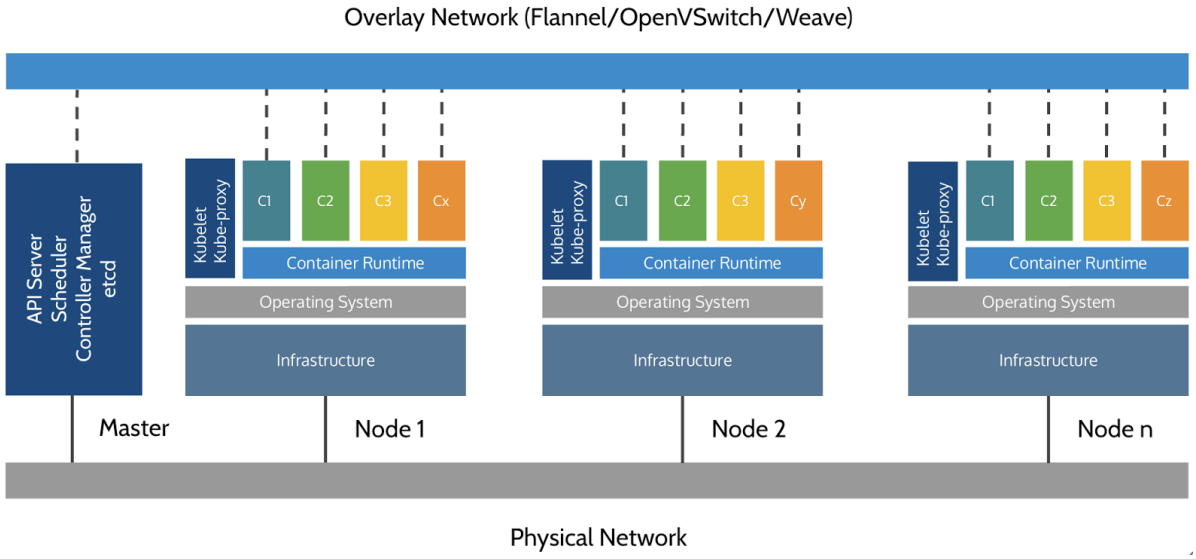
Notion de couches, de registre.

Gestionnaire de conteneur

Docker et alternatives.

Orchestration de conteneurs

Kubernetes, Swarm.



Architecture Kubernetes (K8s)

4. Infrastructure de virtualisation

Le marché de la virtualisation d'entrprise est un marché mature, dynamique et compétitif qui est typiquement dans l'ère du temps.

Les solutions principales proposées sont :

- Des hyperviseurs pour créer des machines virtuelles.
- Les technologies de virtualisation OS (containers ou zones)
- Gestion administrative de la virtualisation serveur (frameworks de base)
- Gestion embarquée de la virtualisation serveur (migration live et automation des fonctions gestion administrative)

Mais c'est sans compter d'autres intérêts d'un plus haut niveau tel que les solutions de backup, de recouvrement de désastre, d'automation avancée, de bureaux virtuels, etc. La virtualisation des architectures x86 occupe aujourd'hui une large place dans les offres des fournisseur de services en nuage.

Les projets open source sont largement représentés par leur sponsors commerciaux.

Par ailleurs, on assiste aujourd'hui à un regain d'intérêt pour la virtualisation software (isolateur) notamment via le projet **docker**.

Une infrastructure virtuelle est constituée de plusieurs éléments eux-mêmes constitué en différentes couches de redondance matérielles ou logiques.

- Infrastructure réseau TCP/IP
- Machines physiques supportant un hyperviseur, machine hôtes hébergeant les VM les invités.
- Stockage local sur l'hôte ou partagé sur le réseau.
- Une interface de gestion accessible en console, via un API tiers ou intégré.

4.1. Réseau TCP/IP et LAN virtuels

Typiquement une infrastructure virtualisée repose sur un ensemble d'éléments interconnectés entre par le réseau en TCP/IP. L'infrastructure physique du réseau doit comporter les mêmes caractéristiques d'évolutivité, de dimensionnement adéquat, de robustesse, de redondance et de fiabilité. Les notions de commutation, de LAN virtuels et de routage sont mis en oeuvre.

4.2. Machine hôte et invités

Les machines physiques sont connectées à une infrastructure commutée et dispose d'un accès au réseau TCP/IP. Ces machines physiques peuvent être construite sur différents types de modèles de serveur en rack ou barebone.

Les hyperviseurs sont hébergés sur des machines hôtes qui exécutent les commandes de machines virtuelles invitées. Les VMs ne sont en fait que des modèles formels d'environnements d'exécution très bien isolés. Les emplacements de stockage ne sont pas virtualisés par l'hyperviseur même s'il peuvent être directement attachés à la machine hôte.

4.3. Stockage

Les emplacements de stockage contiennent :

- les définitions des machines virtuelles (fichiers de configuration)
- ainsi que les disques virtuels utilisés par celles-ci.

On préconisera une infrastructure d'accès au stockage robuste, fiable et évolutive. Des technologies comme iSCSI, FC, LVM ou DRBD sont préconisées. La redondance physique sera assurée par la technologie RAID adaptée.

Catégories de stockage

On trouvera quatre types de stockage :

- **DAS (Direct Attached Storage)**, un emplacement local en général, de type SCSI
- **SAN FC (Storage Area Network en Fiber Channel)**
- Très populaire, **iSCSI** supporté sur de plus en plus de solutions.
- Des protocoles de partage en **NAS (Network Attached Storage)** tels que NFS ou CIFS (Microsoft).

Disques physiques

Ces disques réels doivent être formatés et organisés logiquement. De gros constructeurs disposent de leur solutions fermées. Dans les standards et/ou ouverts, on trouvera iSCSI, LVM, DRBD ou d'autres type de format de données.

Distributions / Appliances Open Source

- Openfiler
- FreeNAS

4.4. Interface de gestion

L'ensemble des ressources (réseau, stockage, CPU/RAM/hosts) peut être administré localement et de manière hétérogène via une interface centrale de gestion accessible à travers une machine cliente du réseau. Citrix XenServer Center ou VMWare Vsphere Center propose ce type de logiciel fonctionnant de manière autonome ou sur une machine de gestion indépendante. Dans le contexte de l'informatique en nuage, on parlera de logiciel d'orchestration, et à d'autres niveaux de « boîtes à outil » et d'API permettant de développer des interfaces tierces.

4.5. Fonctionnalités avancées

Entre autres et sous certaines conditions techniques et financières, ce type d'infrastructure permet au marché de proposer des solutions en terme :

- de snapshots
- de répartition de charge
- de reconfiguration ou de maintenance des hôtes
- de migration ou de mise à jour
- de sauvegarde consolidée
- de plan Disaster Recovery
- de réplication de site
- de supervision et de gestion du réseau et des systèmes
- des migrations P2V (Physique vers Virtuel)
- de réseau virtuel

Pour arriver à ces solutions les acteurs du marché s'associent ponctuellement, publient et utilisent des standards.

4.6. Techniques de migration

De manière sous-jacente ce sont les techniques de migration qui permettent de proposer ces solutions. On trouvera trois techniques de migration appréhendées et gérées par les différents constructeurs de manière différente. On distinguera :

- La relocation froide
- La migration chaude
- La migration live

Fondamentalement, on retiendra que la migration consiste à déplacer de manière cohérente les trois éléments clés d'une VM : CPU/RAM, réseau, et stockage. Ces techniques se distinguent selon la complexité de mise en oeuvre et le temps d'interruption connu.

La relocation froide

But : Déplacer un invité entre des hôtes sans stockage partagé ou avec différentes architectures ou versions d'hyperviseur en encore du P2V.

Processus :

- Arrêter l'invité sur l'hôte source
- Déplacer l'invité d'un système de fichier à un autre (disques de la VM et fichiers de configuration)
- Démarrer l'invité sur l'hôte de destination.

Avantages	Limites
Solutions de maintenance matérielle connaissant l'interruption la plus courte	C'est le processus le plus manuel
Pas de stockage partagé nécessaire	Le service sera interrompu pendant la copie
Les emplacements de stockage peuvent être différents	
La VM originale peut connaître de multiples copies et duplications	

La migration chaude

But : Déplacer un invité entre des hôtes pendant que la disponibilté n'est pas critique.

Processus :

- L'invité se met en pause d'exécution
- L'invité (soit ses fichiers) sont transférés à travers le réseau
- L'invité reprend ses activités sur l'hôte de destination

Avantages	Limites
L'invité et ses applications ne sont pas interrompus	Pendant le temps du transfert, soit assez court, l'hôte ne répondu pas dans l'interface de gestion et sur le réseau
Moins de données à transférer que dans le cas d'une migration live	Nécessite un stockage partagé sur le réseau

La migration live

But : utilisé pour la répartition de charge, la maintenance matérielle et la gestion de l'énergie.

Processus :

- Commence à transférer l'invité en l'état au nouvel hôte.
- Copie à la volée la mémoire RAM de l'invité de manière répétitive (pour assurer la continuité)
- Reconfigure les connexions réseau et l'hôte continue à exécuter ses applications sans interruption du réseau.

Avantages	Limites
Pas d'interruption de service	Nécessiterait un stockage et un réseau partagés
Permanence de la connectivité	L'hôte de destination doit disposer de ressources suffisantes
Bref, disponibilité totale	Les hôtes doivent être configurés de manière similaires

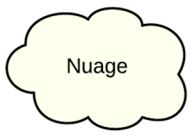
4.7. Apprendre la virtualisation

L'auteur de ces pages a publiés quelques propos sur la virtualisation :

- Virtualisation Linux KVM
- Virtualisation par conteneurs Docker et Kubernetes
- Virtualisation Hyper-V
- Virtualisation VMWare vSphere 6
- OpenStack

5. Impact de l'informatique en nuage

Un nuage : Un nuage représente une infrastructure dont on ne connaît pas vraiment la nature ou la topologie exacte et qui permet d'accéder à un réseau distant. Il s'agit typiquement d'un nuage Internet (au sens propre comme représentant un accès au réseau public) ou d'une simplification dans un diagramme.



Symbole réseau du Nuage

Avec l'informatique en nuage, du trafic d'entreprise pourrait arriver dans des centres de données externes à celle-ci.

Dans le cadre de ce modèle, certains services d'infrastructure se virtualisent jusqu'à être disponibles et utilisés en tant que services. On pensera aux plateformes virtuelles Cisco CSR1000v ou ASAv, ou encore la programmabilité des plateformes IOS XE, notamment en Python. Le modèle de déploiement des infrastructures Wi-fi Cisco Meraki à travers une interface Web sur un serveur chez Cisco est encore un autre exemple. Si on est curieux et informaticien chevronné, on peut déjà prendre un compte sur Cisco Devnet où le "réseau est code".

5.1. Définition du Cloud Computing

Le NIST donne sa définition du Cloud Computing. Le Cloud Computing se définit selon le NIST en 5 caractéristiques essentielles, 3 niveaux de service et 4 modèles de déploiement.

Cinq Caractéristiques Essentielles

1. Un service en libre-service à la demande ;
2. accessible sur l'ensemble du réseau ;
3. avec une mutualisation des ressources ;
4. rapidement élastique (adaptation rapide à une variation à la hausse ou à la baisse du besoin) ;
5. mesurable (mesure et affichage des paramètres de consommation).

Si l'une de ces conditions ne sont pas remplies, il ne s'agit pas d'une technologie qui peut être vendue comme une technologie en nuage.

Trois niveaux de service

Le modèle propose trois niveaux de services qui départagent les responsabilités entre le fournisseur du service en nuage et son client :

1. IaaS : Infrastructure as a Service ; calcul (proc/ram), stockage, réseau ;
2. PaaS : Plateform as a Service ; un stack LAMP par exemple ;
3. SaaS : software as a Service : commander et utiliser un logiciel en ligne (logiciel de facturation, un CRM, une suite bureautique, ...).

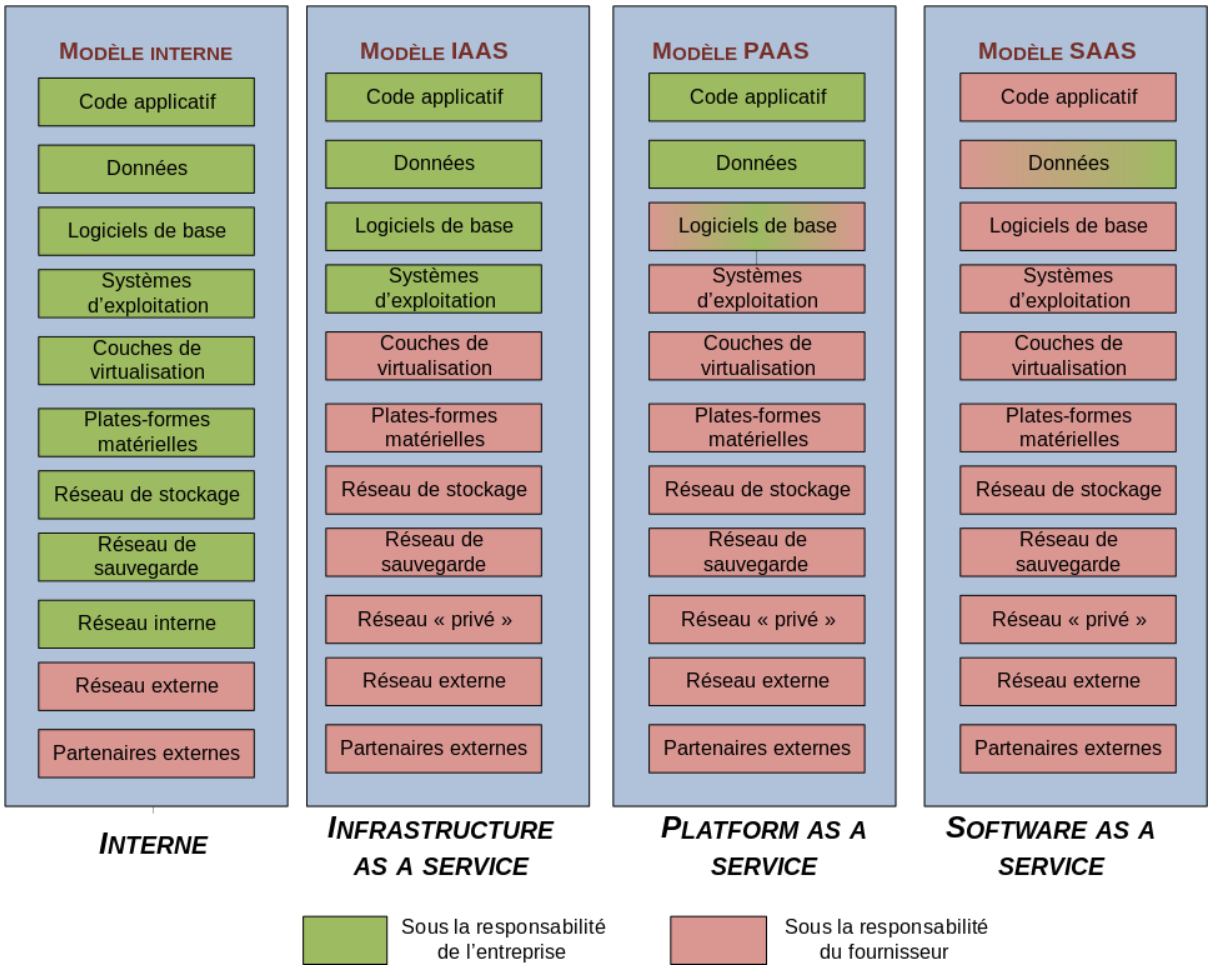
Quatre modèles hiérarchiques de déploiement

1. le nuage public (ouvert au public) ;
2. le nuage privé (pour une même organisation) ;
3. le nuage communautaire (pour une communauté d'utilisateurs ou d'organisations) ;
4. le nuage hybride (plusieurs types de nuages).

5.2. Niveaux de service

Le niveaux de service correpond au niveau de responsabilité[18] ...

18. Source de l'image : Cloud Computing : les différents modèles de services



Cloud Computing : les différents modèles de services

Infrastrustructure as a Service

Définition Infrastrustructure as a Service.

Services de base :

- Calcul (Compute) : virtualisation
- Stockage bloc : pour les images et les mémoires de masse des machines virtuelles
- Commutateur/Routeur/pare-feu virtuel : pour interconnecter les machines virtuelles
- Stockage objet : pour le stockage de fichier

Le Baremetal-as-a-Service définition.

Le dernier Magic Quadrant “Infrastructure as a Service (IaaS) Worlwilde 2019” donne la liste des prestataires mondiaux parmi d’autres plus locaux ou plus spécialisé : AWS, Azure, Google Cloud Plateform (GCP) sont les grands noms à suivre.

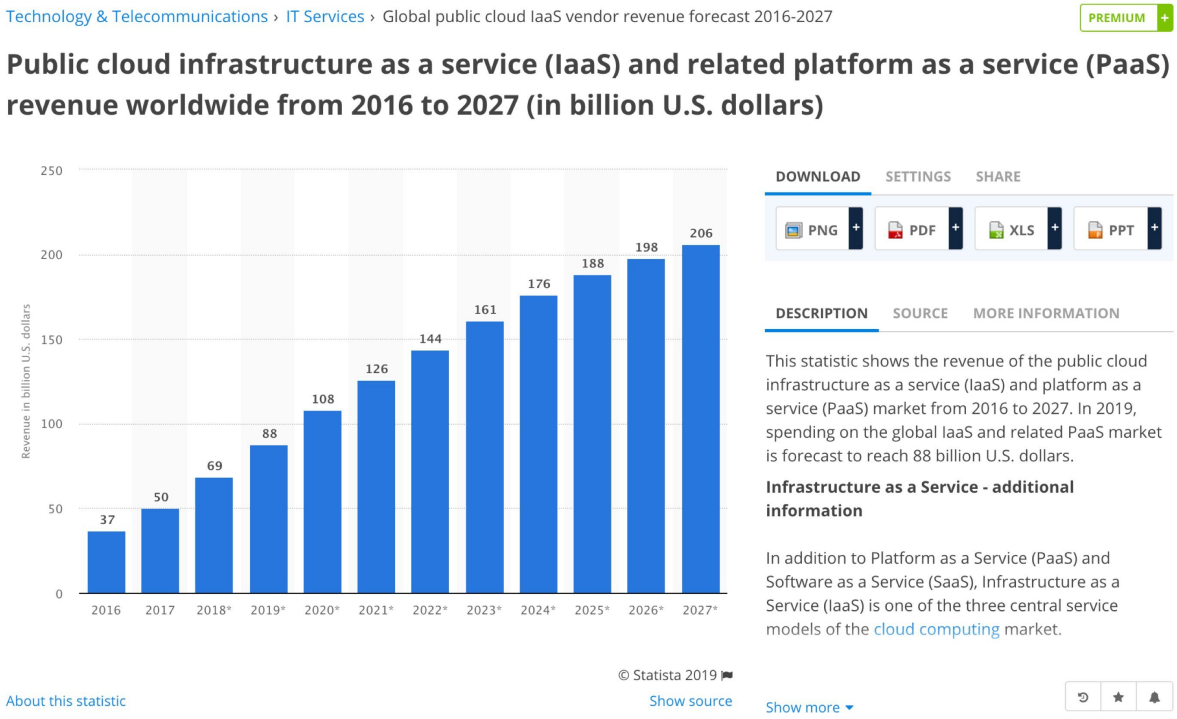
Gartner Magic Quadrant "Infrastructure as a Service (IaaS) Worlwilde 2019"

Beaucoup de critères éléminatoires sont pris en compte :

- ...
- ...

Sources : AWS Named as a Leader in Gartner's Infrastructure as a Service (IaaS) Magic Quadrant for the 9th Consecutive Year, Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, 2019

La taille du marché IaaS devrait croître de manière exponentielle dans les années qui viennent.



Public cloud infrastructure as a service (IaaS) and related platform as a service (PaaS) revenue worldwide from 2016 to 2027 (in billion U.S. dollars)

Source : Public cloud infrastructure as a service (IaaS) and related platform as a service (PaaS) revenue worldwide from 2016 to 2027 (in billion U.S. dollars), Statista

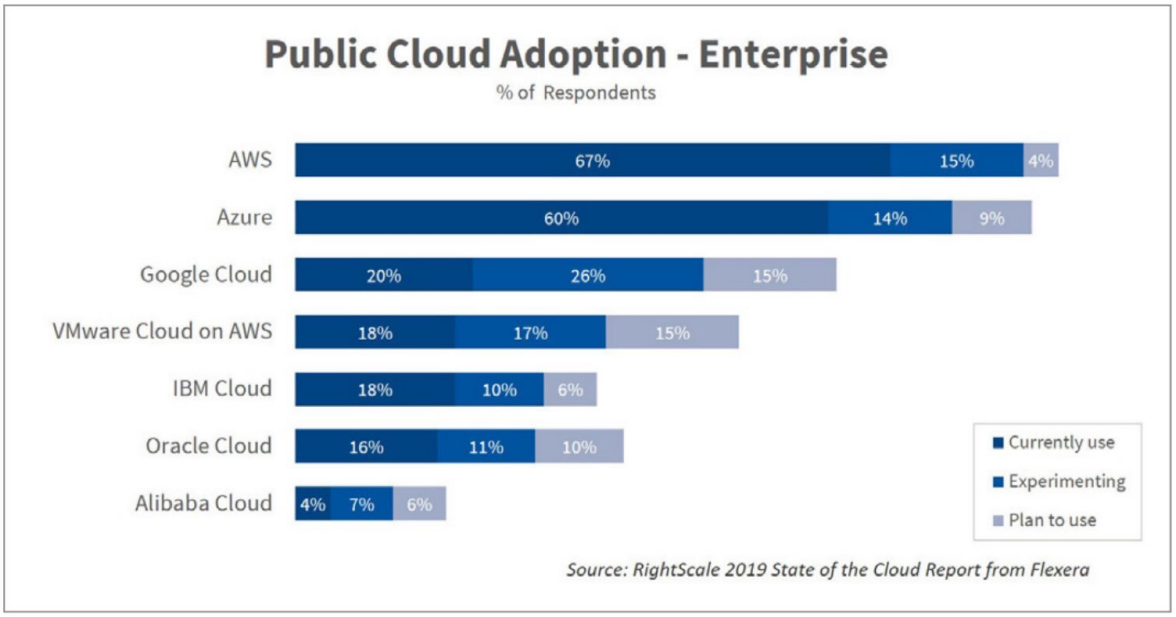
Container-as-Service

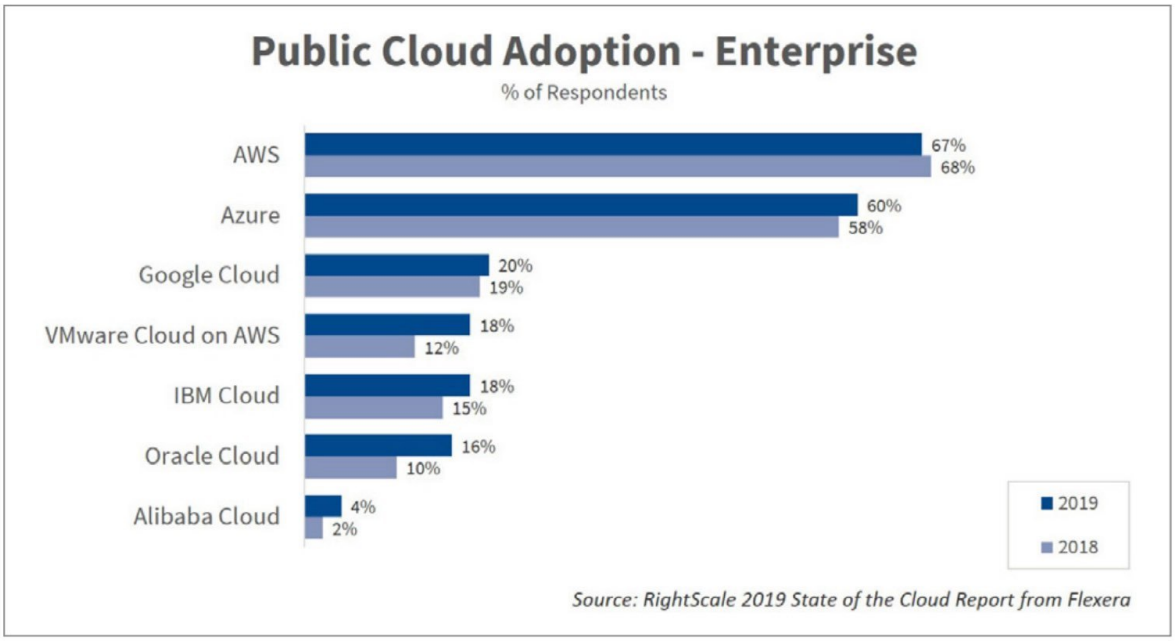
Middelware. PaaS.

- Container-as-a-service
- Container-registrey-as-service
- Kubernetes-as-service
- Function-as-a-Service

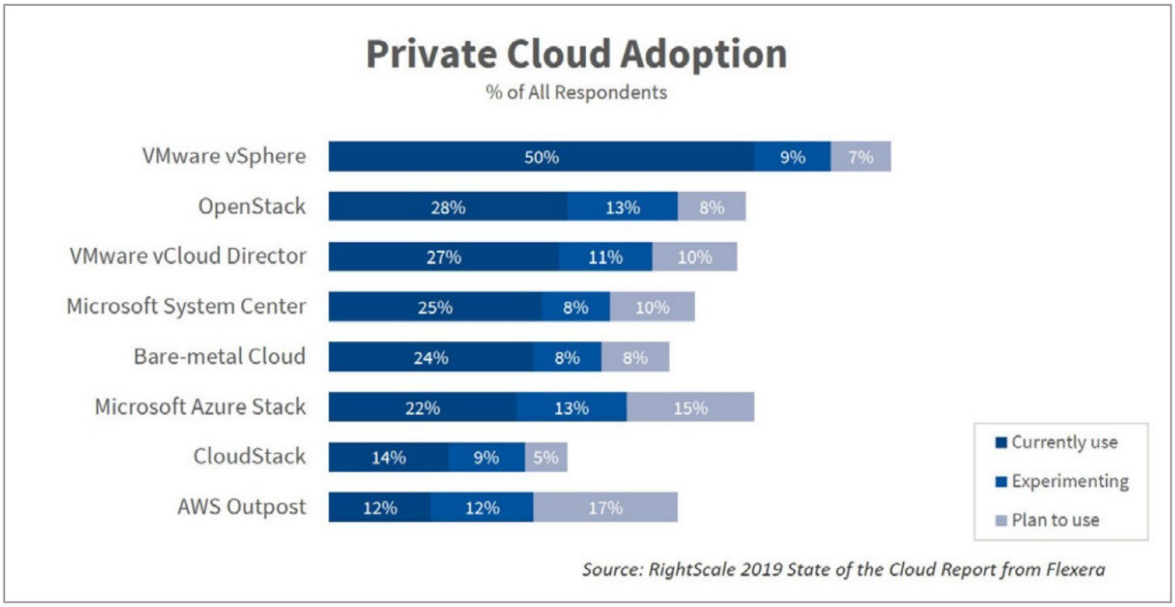
5.3. Offres publiques et solutions privées

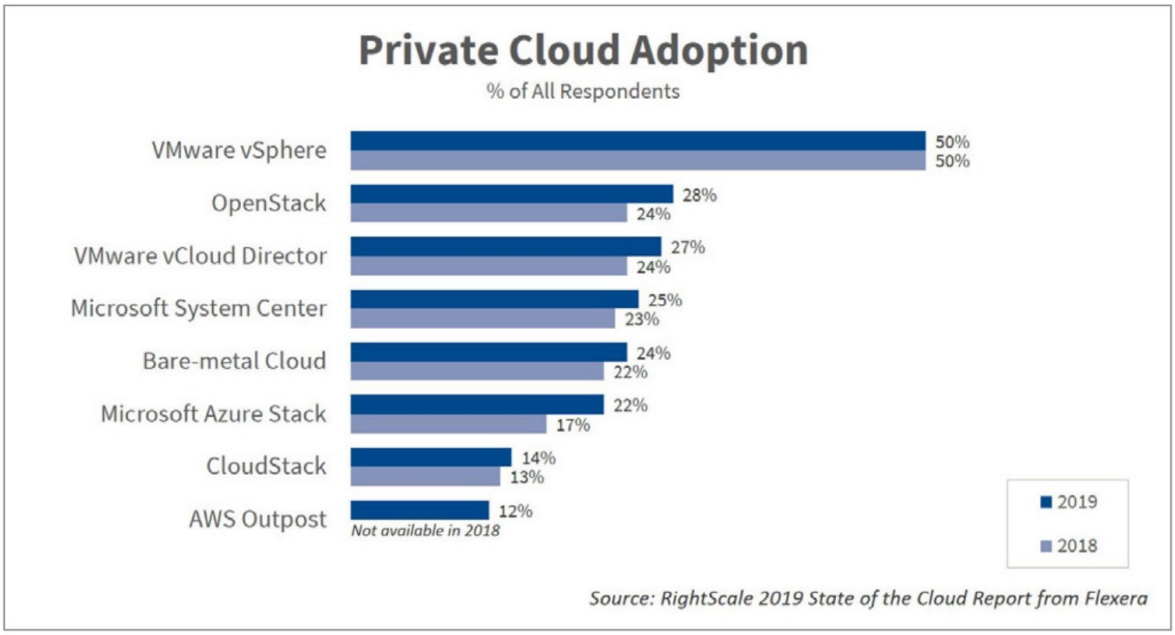
Source : RightScale 2019 State of the Cloud-Report from Flexera





Public Cloud Adoption, RightScale 2019 State of the Cloud-Report from Flexera





Private Cloud Adoption, RightScale 2019 State of the Cloud-Report from Flexera

5.4. Ressources nécesaires en connectivité

Quatre services techniques[19] sont essentiels pour supporter un haut niveau de flexibilité, de disponibilité des ressources et en transparence des ressources en connectivité indispensables au *cloud computing* :

- Le réseau L3 offre des interconnexions habituelles entre sites distants et fournit un accès au cloud au utilisateurs finaux.
- Le “LAN étendu” entre deux ou plusieurs sites offre un transport transparentet supporte la mobilité des applications et des systèmes d’exploitation.

19. https ://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-xr-software/white_paper_c11-694882.html

- Un service “SAN étendu” assure l’accès aux données et la réplication de données.
- La localisation IP améliore le trafic “northbound” et “southbound” autant que les flux serveur-à-serveur.

5.5. Impact sur les opérations réseau

On notera au moins deux impacts pour ceux qui s’occupent des infrastructures réseaux.

D’une part, les architectures de conception seront modifiées au profit d’une séparation stricte entre le plan des données et le plan de gestion.

D’autre part, le plan de gestion sera notamment accessible non plus via des consoles physiques ou virtuelles dédiées à chaque périphérique mais via une couche supplémentaire supportée par un “contrôleur”. Ce dernier dispose d’une interface API REST qui facilite la mise en forme de code (le codage) des infrastructures notamment grâce à l’usage du protocole HTTP et d’un langage de programmation comme Python.

5.6. Infrastructure as a Code (IAC)

“L’infrastructure en tant que code (IAC) est un type d’infrastructure informatique que les équipes d’exploitation peuvent automatiquement gérer et provisionner via du code, plutôt que d’utiliser un processus manuel. L’infrastructure en tant que code est parfois appelée infrastructure programmable.”[20]

5.7. SDN et NFV

On distinguera les deux concepts d’architecture SDN et NFV.

- **SDN (Software Defined Network)** : architecture qui sépare physiquement le plan de contrôle du plan de transfert de données et dans laquelle le plan de contrôle dirige plusieurs périphériques. ONF, SDN Definition.
- **NFV (Network Functions Virtualization)** : est une architecture qui utilise des technologies de virtualisation pour gérer des fonctions essentielles du réseau grâce à des logiciels plutôt qu’avec du matériel. Le concept NFV se fonde sur des blocs de fonctions vitualisées du réseau qui peuvent être combinées pour fournir un service réseau sur mesure et évolutif. Concrètement, ces fonctions sont exécutées par des machines virtuelles au dessus du matériel ; ce sont des routeurs, des switches, des serveurs ou des systèmes de cloud computing. Les fonctions proposées sont la sécurité et le pare-feu, le NAT, le DNS, les caches , des services de détection d’intrusion (IDS), etc. NFV – Network Functions Virtualization

NFV et SDN utilisent tous les deux une couche d’abstraction. Alors que SDN cherche à séparer le contrôle et le transfert, NFV met une couche d’abstraction dans les fonctions de transfert du réseau (et autres) assurés par du matériel. Les deux concepts s’implémentent de manière complémentaires mais existent aussi indépendamment l’un de l’autre.

5.8. Architecture Network Virtualization

Une architecture “Network virtualization” est composée de trois éléments :

- **Network access control and segmentation of classes of users** : “Users are authenticated and either allowed or denied into a logical partition. Users are segmented into employees, contractors and consultants, and guests, with respective access to IT assets. This component identifies users who are authorized to access the network and then places them into the appropriate logical partition.”

20. Paradigme Infrastructure as a Code : “*Infrastructure as Code (IAC) is a type of IT infrastructure that operations teams can automatically manage and provision through code, rather than using a manual process. Infrastructure as Code is sometimes referred to as programmable infrastructure.*” (What is Infrastructure as Code (IAC) ? - Definition from WhatIs.com)

- **Path isolation** : “Network isolation is preserved across the entire enterprise : from the edge to the campus to the WAN and back again. This component maintains traffic partitioned over a routed infrastructure and transports traffic over and between isolated partitions. The function of mapping isolated paths to VLANs and to virtual services is also performed in component.”

- **Network Services virtualization** : “This component provides access to shared or dedicated network services such as security, quality of service (QoS), and address management (Dynamic Host Configuration Protocol [DHCP] and Domain Name System [DNS]). It also applies policy per partition and isolates application environments, if required.”

Références :

http ://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11-531522.pdf

https ://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11-531522.html

5.9. APIs

Un API, interface de programmation applicative (application programming interface), est une méthode d’échange de données d’une application avec une autre. Bien que l’on se réfère au terme “interface”, il s’agit d’interfaces logicielles et non matérielles.

Les méthodes et protocoles suivants sont des sortes d’API, soit des interfaces de gestion :

- API HTTP REST
- SSH
- SNMP, CDP
- Openflow

Quatrième partie Technologies WAN

Cette partie présente les technologies WAN et leur évolution. La présentation et la configuration des protocoles PPP, MLPPP, PPPoE avec les authentifications CHAP/PAP, du protocole de tunnel GRE et du protocole de routage extérieur BGP sont des sujets WAN.

4. Technologies et topologies WAN

1. Technologies WAN

Les technologies WAN sont considérées comme des technologies d'accès au réseau (L2) positionnées physiquement (HDLC, Ethernet) et/ou logiquement (PPP, IP/MPLS, IPSEC, TLS, HTTPS).

Elles sont utilisées pour un accès :

1. soit, à un WAN privé qui interconnecte des sites distants ;
2. soit, à l'Internet (WAN public)
    - afin d'accéder à des ressources publiques
    - ou afin d'accéder à des ressources privées éventuellement via des tunnels VPN

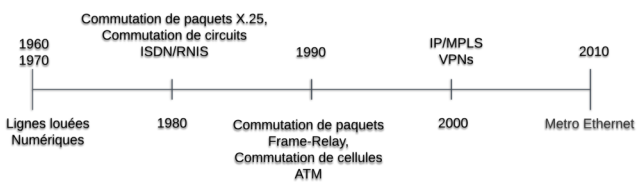
et de manière optionnelle avec des services de sécurité qui assurent des niveaux de confidentialité, d'authentification et d'intégrité.

Les technologies WAN sont diverses dans le monde pour des accès et dans les infrastructures des opérateurs. Les acronymes suivants désignent certaines de ces technologies.

- Metro ethernet
- VSAT
- Cellulaire 3g/4g
- IP MPLS
- T1/E1
- ISDN / RNIS
- xDSL, PPPoE
- Frame-Relay
- Cable DOCSIS
- VPN : IPSEC, DMVPN, VPN TLS

1.1. Généalogie des technologies WAN

Les technologies évoluent depuis bien plus longtemps que les technologies TCP/IP.



Généalogie des technologies WAN depuis le milieu du XXe siècle

1.2. Entreprise Internet Access

- Broadband PPPoE
- Internet DSL Link
- DOCSIS Cablo-opérateurs
- Wireless ISP

1.3. Options de connectivité WAN privé

- Metro Ethernet
- IP MPLS
- Les technologies VPN

1.4. Etablissement de circuit

Commutation de circuit

La commutation de circuit est un mode d'établissement d'une liaison de télécommunication pour laquelle :

- un **chemin** physique ou logique est établi entre deux équipements

et

- est **bloqué** pour toute la durée de la communication.

L'établissement de circuit est aujourd'hui exécutée de manière électronique.

Dans la commutation par circuit, il y a un risque de sous-utilisation du support en cas de "silence" pendant la communication.

RNIS (ISDN) est un exemple de technologie à commutation de circuit qui numérise la voix en tant que service.

Avec la commutation par circuit, le temps passé est facturé.

Commutation de paquet

La commutation de paquets s'oppose au principe de la commutation de circuit. La commutation de paquets optimise le canal de transmission laissant le soin à des commutateurs intermédiaires de placer et d'acheminer les paquets (Ethernet, Wi-Fi, IP) ou en établissant des Circuits Virtuels (ATM, Frame-Relay) sur des infrastructures sous-jacentes.

Ces technologies sont facturées par quantité de données échangées.

Le protocole MPLS permet de construire des réseaux IP cohérents sur ces architectures préexistantes avec une forme de confidentialité et de la gestion de qualité de service.

1.5. Couche physique

- Cuivre
- Fibre optique
- Ondes radios

2. Options de connectivité WAN vers l'Internet

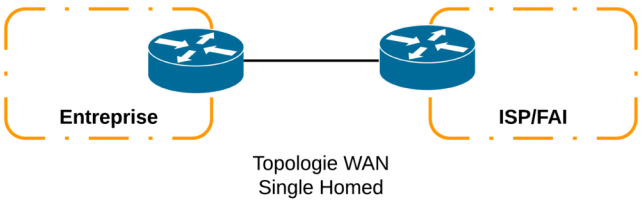
Les technologies peuvent se caractériser par le nombre de connexion auprès d'un seul ou plusieurs fournisseurs de services. Ce type de connectivité assure une redondance vers les services externes à l'organisation.

- **Single Homed** : Connexion unique auprès d'un FAI/ISP.
- **Dual Homed** : Double connexion auprès d'un seul FAI/ISP.
- **Single Multihomed** : Une seule connexion auprès de 2+n FAI/ISP.
- **Dual Multihomed** : Double connexion auprès de 2+n FAI/ISP.

.	Homed	Multihomed
Single	Une seule connexion auprès d'un seul FAI/ISP.	Une seule connexion auprès de 2+n FAI/ISP.
Dual	Double connexion auprès d'un seul FAI/ISP.	Double connexion auprès de 2+n FAI/ISP.

2.2. Connectivité Single Homed

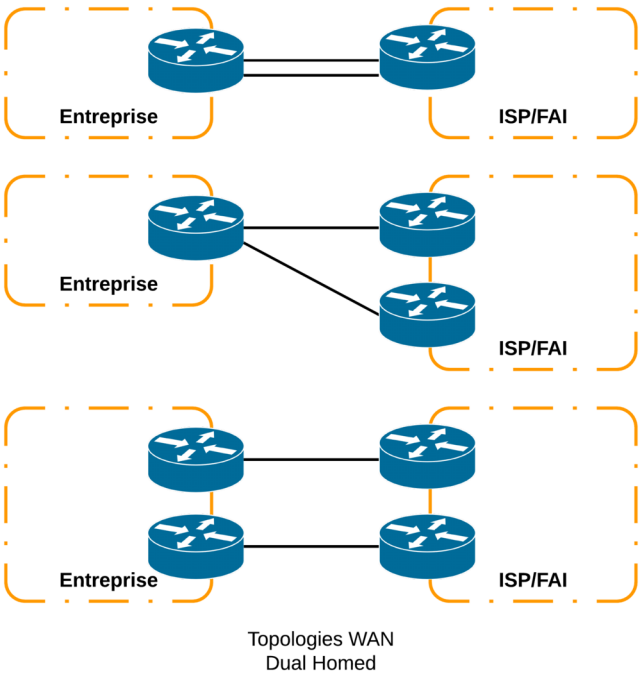
Dans une topologie Single Homed, il y a une connexion unique auprès d'un FAI/ISP.



Single Homed : Connexion unique auprès d'un FAI/ISP.

2.3. Connectivité Dual Homed

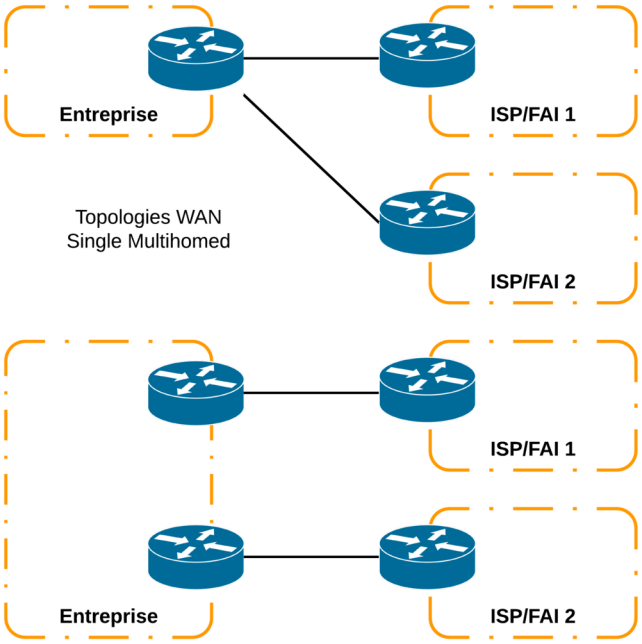
Avec une connectivité "Dual Homed", il y a une double connexion vers le fournisseur d'accès Internet quel que soit le nombre de routeur chez le client ou le fournisseur.



Dual Homed : Double connexion auprès d'un seul FAI/ISP.

2.4. Connectivité Single Multihomed

Dans une topologie "Single Multihomed", on trouvera une seule connexion vers plusieurs fournisseurs d'accès Internet, quel que soit le nombre de routeurs nécessaires chez le client.

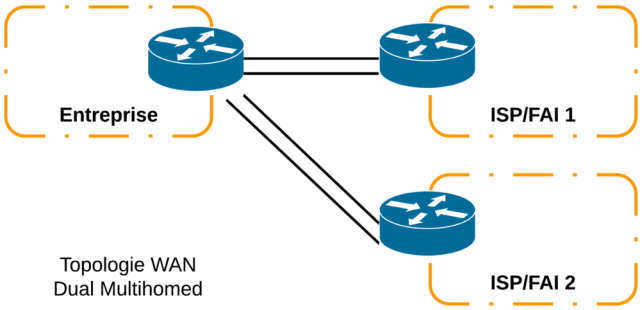


Single Multihomed : Une seule connexion auprès de 2+n FAI/ISP.

2.5. Connectivité Dual Multihomed

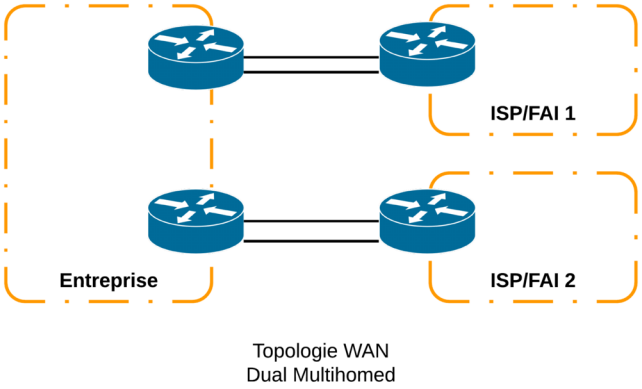
Dans une topologie "Dual Multihomed" on trouvera une double connexion vers plusieurs fournisseurs d'accès à Internet quel que soit le nombre et les liaisons établies de chaque côté.

Dans la figure suivante, on trouve une double connexion vers plusieurs fournisseurs d'accès à Internet à partir d'un seul noeud chez le client.



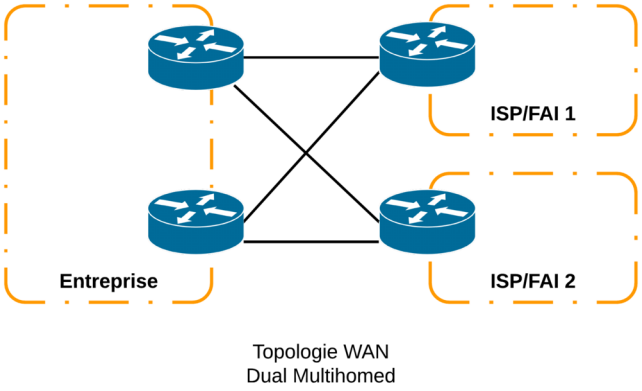
Double connexion vers plusieurs FAI à partir d'un seul noeud

Dans la figure suivante, on trouve une double connexion vers plusieurs fournisseurs d'accès à Internet à partir de deux noeuds dédiés à chacun chez le client.



Double connexion vers plusieurs FAI à partir de deux noeuds

Dans la figure suivante, on trouve une double connexion vers plusieurs fournisseurs d'accès à Internet à partir de deux noeuds chez le client qui réalise un maillage entre les deux côtés.



Double connexion vers plusieurs FAI à partir de deux noeuds avec maillage

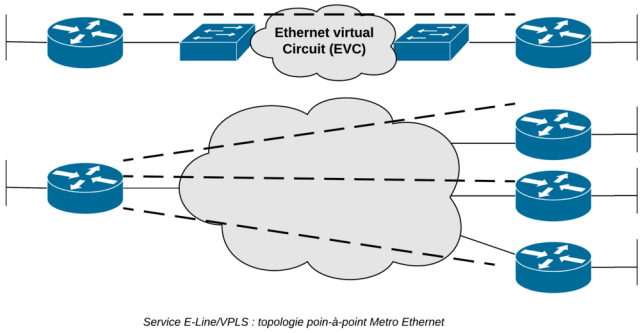
3. Metro Ethernet (MetroE)

- http ://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/Ethernet_Access_for_NG_MAN_-WAN_V3-1_external.html

- https ://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-Layer2WANDesignGuide-AUG14.pdf
- http ://searchsdn.techtarget.com/opinion/How-software-defined-networking-will-boost-carrier-Ethernet-services

3.1. Connectivité Point-to-Point : Service E-Line/VPLS

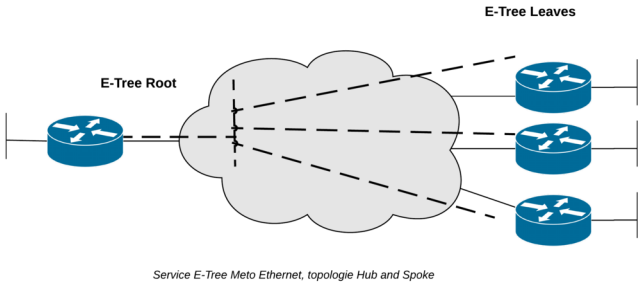
Connexions point-à-point.



Connexions point-à-point

3.2. Connectivité Hub-and-Spoke : Service E-Tree

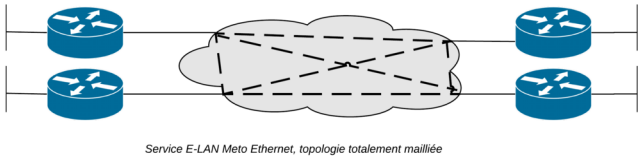
Topologie Hub and Spoke.



Topologie Hub and Spoke

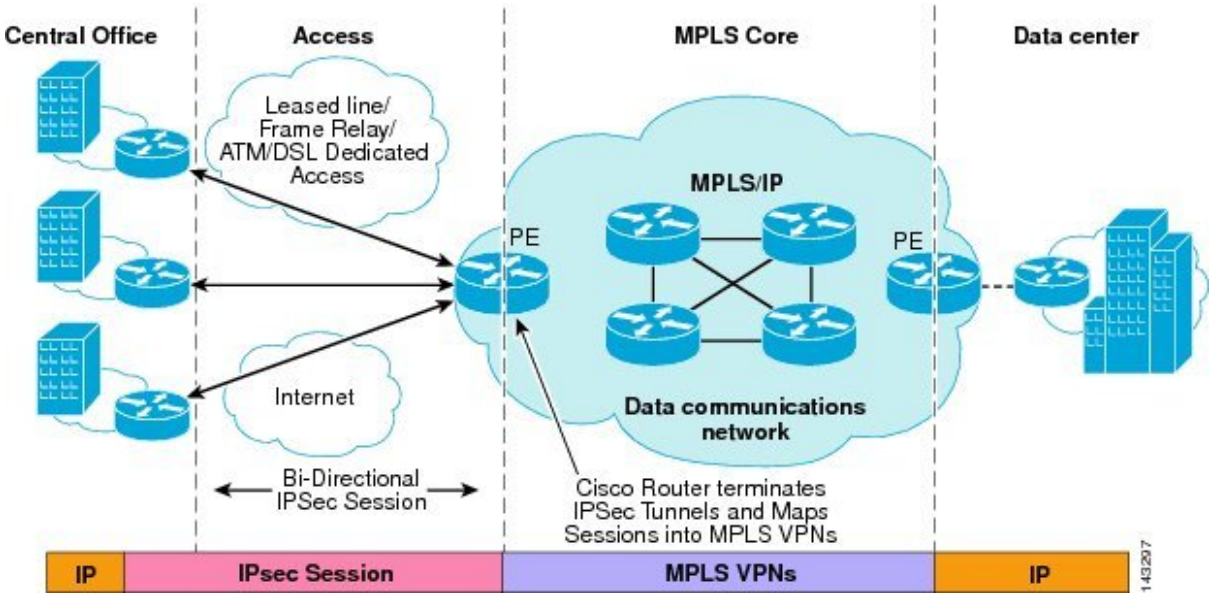
3.3. Connectivité Mesh : Service E-LAN

MetroE Ethernet E-LAN Service : topologie maillée.



MetroE Ethernet E-LAN Service

4. Architecture IP / MPLS



Architecture IP / MPLS

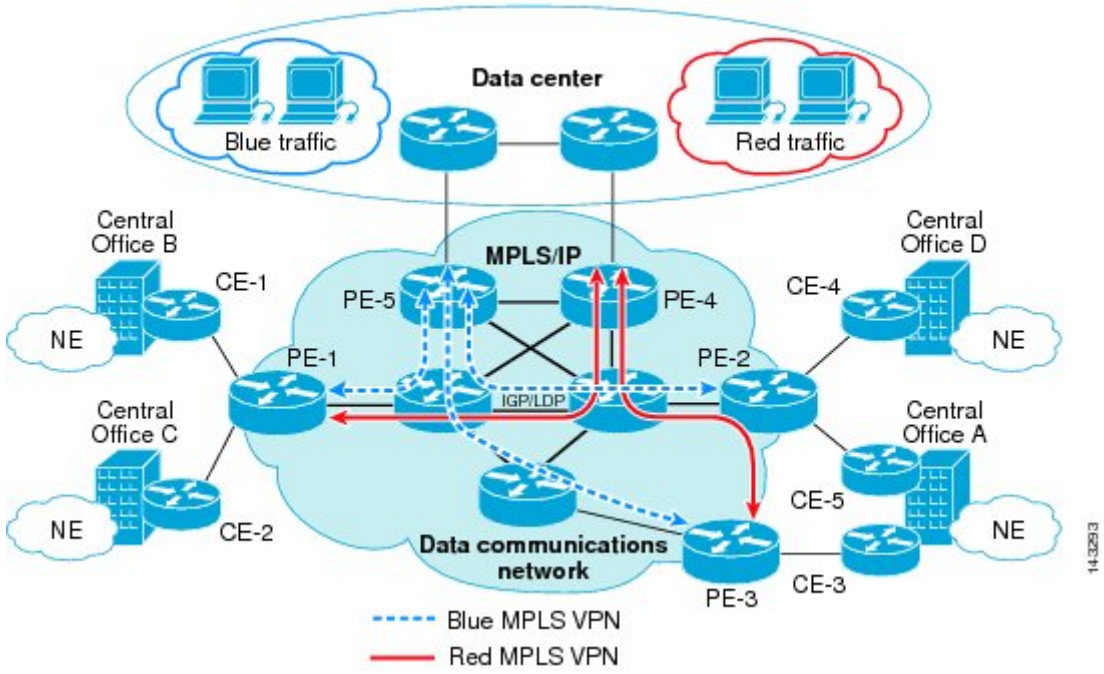
MultiProtocol Label Switching (MPLS) est un mécanisme de transport de données basé sur la commutation d'étiquettes ou "labels", qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie. À l'origine, cette insertion s'opère entre la couche de liaison de données (niveau 2) et la couche réseau (niveau 3) afin de transporter des protocoles comme IP. C'est pourquoi de temps à autres **MPLS est qualifié de protocole de couche "2,5"**, entre la couche 2 (L2) du modèle OSI et la couche 3 (L3).

Ce protocole a évolué pour fournir un service unifié de transport de données pour les clients en utilisant une technique de commutation de paquets. MPLS peut être utilisé pour transporter pratiquement tout type de trafic, par exemple la voix ou des paquets IPv4, IPv6 et même des trames Ethernet ou ATM.

MPLS permet d'acheminer sur une seule infrastructure différents types de trafic dissociés tout en respectant les contraintes de fonctionnement associées.

Comme son sigle (MPLS) l'indique, ses caractéristiques sont :

- **multiprotocol** (multi-protocoles) : il est capable de supporter les différents protocoles de niveau inférieur, au sens OSI (ATM, Frame relay…)
- **label switching** (commutation par étiquettes) : il se base sur une étiquette (en anglais : label) ou identifiant pour la commutation des paquets. Cette étiquette est attribuée aux paquets par l'équipement PE (Provider Edge) lors de leur entrée dans l'infrastructure MPLS.

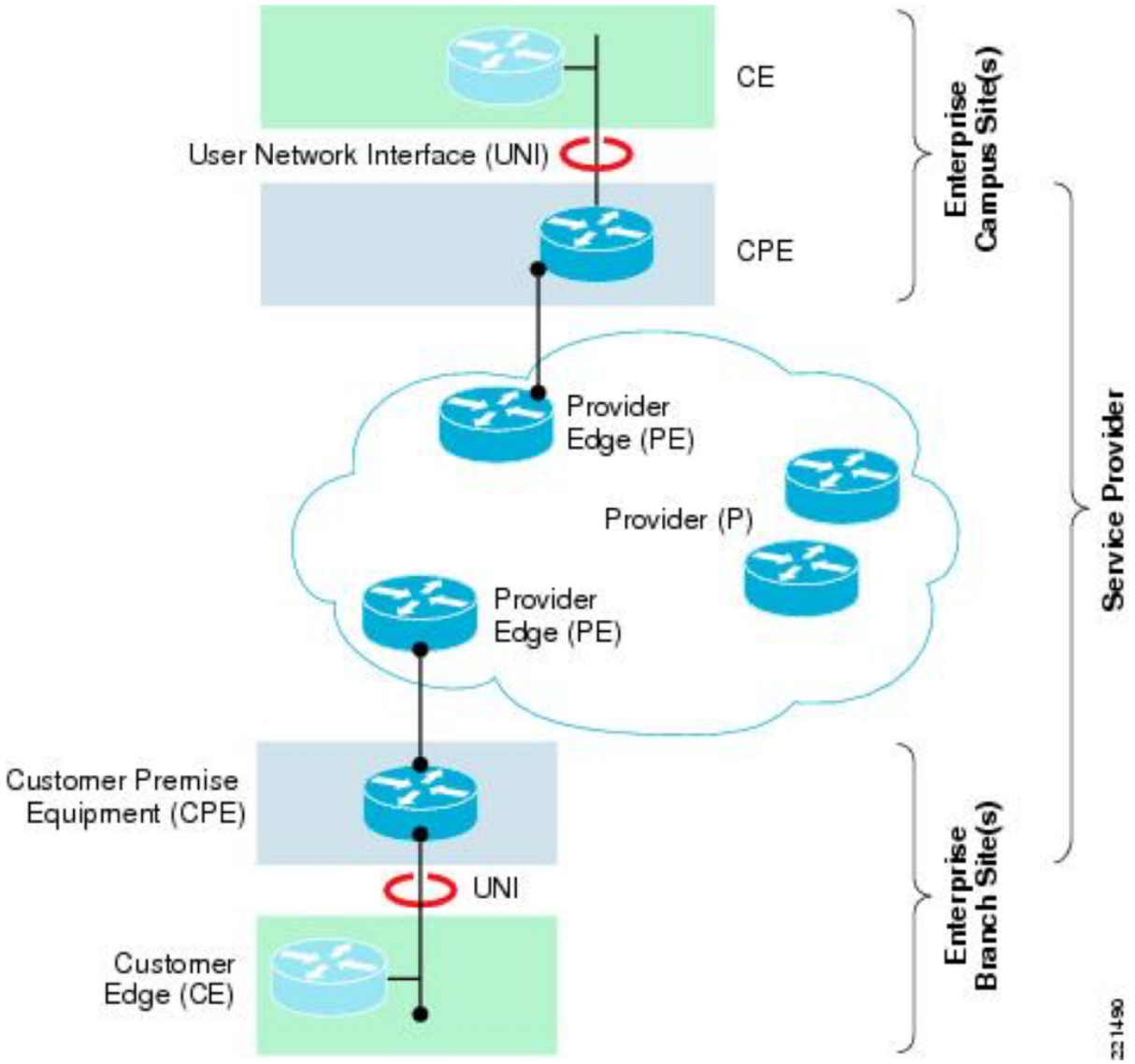


Toplogie IP MPLS

Sources : http ://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/telco_dcn/Book/telco5.html et https ://fr.wikipedia.org/wiki/Multi Label_Switching

Terminologie IP MPLS

- **CE Customer Edge** : Équipement du client.
- **CPE Customer Premises Equipment** : Équipement du client (ou du FAI) qui donne accès au nuage opérateur.
- **UNI User Network Interface** : Interface d'accès au nuage opérateur qui détermine la frontière des responsabilités.
- **PE Provider Edge** : Premier matériel actif du nuage opérateur.
- **P Provider** : Equipement dans le nuage opérateur que le client ignore.



Terminologie IP MPLS

Source : http ://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/Ethernet_Access_for_NG_-MAN_WAN_V3-1_external.html

5. Solutions WAN privé VPN

5.1. Définition d'un VPN

Un réseau privé virtuel virtual private network (VPN) étend un réseau privé à travers un réseau public comme l'Internet.

Il permet à un ordinateur d'envoyer et de recevoir des données à travers des réseaux partagés ou publics comme s'ils étaient directement connectés au réseau privé, tout en bénéficiant des fonctionnalités, de la sécurité et des politiques de gestion de ce réseau privé.

Une liaison VPN est créée en établissant une connexion virtuelle point à point sur de véritables connexions physiques par des protocoles de mise en tunnel et/ou de chiffrement du trafic.

Un VPN n'est pas nécessairement "sécurisé", on peut le considérer comme une facilité d'accès (*Virtual Network*) offrant le service d'une "ligne physique privée" (*Private*) (soit pas nécessairement confidentielle ou authentique).

5.2. Avantages

Les technologies VPN permettent de connecter des endroits à travers le monde de manière sécurisée et cohérente.

Aussi, les accès distants pour les utilisateurs mobiles connaissent son succès.

Enfin, les utilisateurs domestiques peuvent utiliser ces technologies pour cacher leur présence sur Internet.

5.3. Catégories

Les VPNs peuvent être dans des modèles :

- à accès distant (remote-access, road-warrior) connectant des individus à un réseau privé, établis à la demande
- site-à-site (site-to-site) connectant deux réseaux en leur bordure

Les systèmes VPN peuvent être classés selon :

- les protocoles utilisés pour la mise en tunnel du trafic
- le point de terminaison du tunnel
- la connectivité “site-to-site” ou “remote-access”
- le niveau de sécurité offert
- la couche OSI présente dans la connexion : des circuits de type L2 ou une connectivité réseau de type L3
- l’usage : WAN privé, WAN public

5.4. VPN non sécurisés

Toute encapsulation peut embarquer un paquet IP. En ce sens, tout protocole, quelle que soit sa couche pourrait servir de protocole de tunnel et servir de facilité VPN non sécurisé (ou sécurisé).

On connait des cas comme ip-in-ip, 6in4, et … GRE pour des protocoles de tunnels à usage en général légitime.

Il est trivial de placer du trafic IP dans des paquets ICMP, DNS ou TLS sur le port 443 qui sont difficilement ou négligemment filtrés par les pare-feu et les proxys en sortie.

5.5. VPN sécurisés

Les technologies VPN peuvent supporter des protocoles et des algorithmes de chiffrement, d’authentification et d’intégrité.

Un modèle de sécurité VPN assure :

- La confidentialité : même si le trafic est capturé, l’attaquant ne verra que du trafic chiffré
- L’authentification de l’émetteur pour empêcher des accès non autorisés
- L’intégrité des messages afin de détecter leur altération

5.6. VPN IPSEC Site-to-Site

Internet Protocol Security (IPsec) a été initialement développé par l’IETF pour IPv6 (quand celui-ci était obligatoire jusqu’au RFC 6434 qui se contente désormais de le recommander).

IPsec est un protocole standard de sécurité largement déployé avec IPv4 et L2TP. Attention, il s’agit d’un “framework” ouvert composé de plusieurs protocoles et supportant divers algorithmes.

Sa conception rencontre les objectifs principaux de la sécurité : authentification, intégrité et confidentialité. IPsec utilise le chiffrement en encapsulant les paquets IP dans un paquet IPsec. Il opère donc à la couche 3. La désencapsulation intervient en bout du tunnel pour rendre le paquet IP original.

5.7. VPN TLS (Remote Access)

Transport Layer Security (TLS) est un protocole de couche applicative qui peut mettre en tunnel le trafic entier d'un réseau ou des connexions individuelles.

On peut aussi lui trouver des fonctionnalités de type "WebVPN". Un grand nombre de fabricants propose des solutions d'accès distants par VPN toutes aussi incompatibles entre elles.

Enfin, un VPN TLS peut se connecter quasiment de n'importe quel endroit là où IPsec peut poser des problèmes avec les règles de pare-feu et NAT.

5.8. Cisco Dynamic Multipoint VPN (DMVPN)

Cisco Dynamic Multipoint VPN (DMVPN) simplifie les configurations VPN en utilisant les protocoles : * GRE : Generic Routing Encapsulation (RFC 2784) * NHRP : Next Hop Resolution Protocol (protocole IETF) * IPSEC

Topologies DMVPN

On trouvera deux types de topologies VPN :

- Dual hub-dual DMVPN cloud
- Dual hub-single DMVPN cloud

Source : https ://supportforums.cisco.com/sites/default/files/legacy/3/9/5/26593-DMVPNbk.pdf

5.9. Autres protocoles VPN sécurisés

- Datagram Transport Layer Security (DTLS) - utilisé par Cisco AnyConnect VPN et par OpenConnect VPN pour résoudre un problème TLS avec les tunnels sur UDP.
- Microsoft Point-to-Point Encryption (MPPE) fonctionnant avec Point-to-Point Tunneling Protocol et d'autres implémentations
- Multi Path Virtual Private Network (MPVPN).
- Secure Shell (SSH) VPN - OpenSSH
- PPTP/L2TP

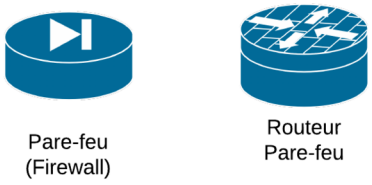
Cinquième partie Filtrage pare-feu et IDS

Dans cette partie, on exposera les concepts fondamentaux des pare-feu (Firewall) ainsi que des descriptions du marché des pare-feu, Firewall NG ou UTM. Un pare-feu (Firewall) réalise un filtrage du trafic sur des éléments de couche 3 (L3) et couche 4 (L4). On proposera un exercice de mise en oeuvre de la fonctionnalité Cisco IOS ZBF (Zone Based Firewall). On y démontrera que le NAT ne sécurise en rien le réseau. On y apprendra aussi à mettre en place de politiques de filtrage entre des zones LAN, DMZ, Internet et le pare-feu lui-même (Self). Enfin, on terminera cette partie par l'exposé des concepts IDS et IPS, objets connexes aux pare-feu dans le rôle de filtrage de sécurité des réseaux. Enfin, on terminera le chapitre en évoquant le sujet "Cisco Switched Port Analyzer (SPAN)" qui permet de capturer du trafic qui traverse des VLANs ou des ports de commutateur à partir d'un port tiers. Par exemple, on y place alors une station avec logiciel de capture ou un IDS/IPS.

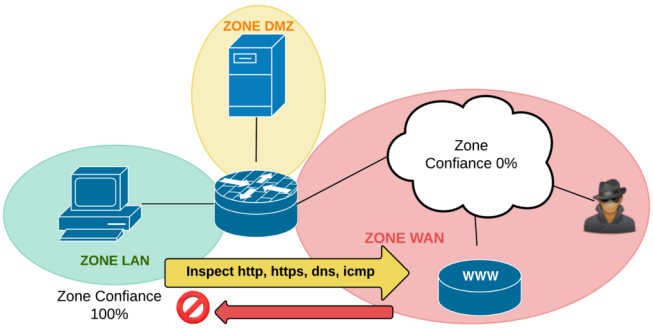
5. Concepts Pare-feu Firewall

1. Introduction au concept de pare-feu

Un **pare-feu** (*firewall*) protège des tentatives de connexion directe venant d'un réseau comme Internet. Par contre, il laisse entrer le retour légitime du trafic initié d'une zone de confiance comme un LAN. Il tient compte de l'état des sessions de couche 4 établies (TCP, UDP, ICMP, etc.). On parle alors de pare-feu à état.



Symboles pare-feu firewall



Topologie pare-feu avec DMZ

Quelques éléments essentiels sont à retenir concernant les pare-feux

- Dans un système d'information, les politiques de filtrage et de contrôle du trafic sont placées sur un matériel ou un logiciel intermédiaire communément appelé pare-feu (*firewall*).
- Cet élément du réseau a pour fonction **d'examiner et filtrer le trafic qui le traverse**.
- On peut le considérer comme une **fonctionnalité** d'un réseau sécurisé : la fonctionnalité pare-feu
- L'idée qui prévaut à ce type de fonctionnalité est le **contrôle des flux du réseau TCP/IP**.
- Le pare-feu limite le taux de paquets et de connexions actives. Il reconnaît les flux applicatifs.
- Se placer au milieu du routage TCP/IP, il fait office de routeur
- Il agit au minimum au niveau de la couche 4 (L4) mais il peut inspecter du trafic L7 (Web Application Firewall)
- Il ne faut pas le confondre avec le routeur NAT

2. Objectifs d'un pare-feu

Il a pour objectifs de répondre aux menaces et attaques suivantes, de manière non-exhaustive :

- Usurpation d'identité
- La manipulation d'informations
- Les attaques de déni de service (DoS/DDoS)
- Les attaques par code malicieux
- La fuite d'information
- Les accès non-autorisé (en vue d'élévation de privilège)
- Les attaques de reconnaissance, d'homme du milieu, l'exploitation de TCP/IP

3. Ce que le pare-feu ne fait pas

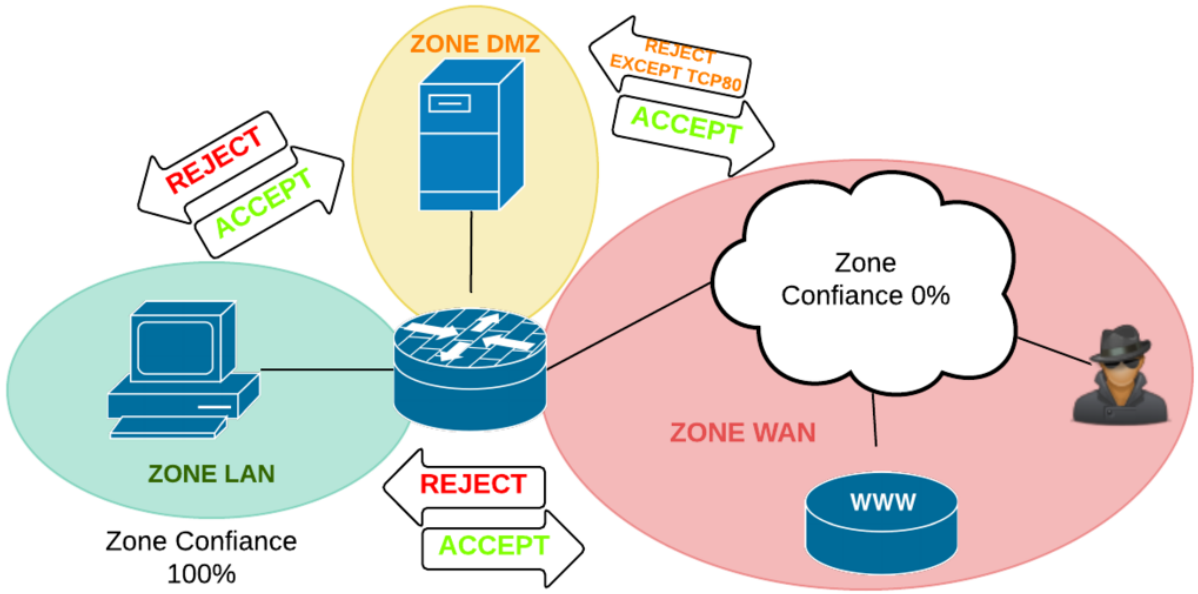
Le pare-feu est central dans une architecture sécurisée mais : * Il ne protège pas des menaces internes. * Il n'applique pas tout seul les politiques de sécurité et leur surveillance. * Il n'établit pas la connectivité par défaut. * Le filtrage peut intervenir à tous les niveaux TCP/IP de manière très fine.

4. Fonctionnement

- Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent.
- Généralement, les zones de confiance incluent l'Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante).
- Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège.
- Un pare-feu fait souvent office de routeur et permet ainsi d'isoler le réseau en plusieurs zones de sécurité appelées zones démilitarisées ou DMZ. Ces zones sont séparées suivant le niveau de confiance qu'on leur porte.

5. Zone de confiance sur un pare-feu

Un organisation du réseau en zones composées d'interfaces permet d'abstraire les règles de filtrages.



Zones de confiance

À titre d'exemple, les politiques de filtrage des applications pourrait être facilement mis en oeuvre quelque soit le protocole de transport IPv4 ou IPv6.

Aussi les politiques de sécurité appliquée sur les pare-feux sont alors plus lisibles, plus faciles à auditer et à gérer.

6. Niveau de confiance

- Le niveau de confiance est la certitude que les utilisateurs vont respecter les politiques de sécurité de l'organisation.
- Ces politiques de sécurité sont édictées dans un document écrit de manière générale. Ces recommandations touchent tous les éléments de sécurité de l'organisation et sont traduites particulièrement sur les pare-feu en différentes règles de filtrage.
- On notera que le pare-feu n'examine que le trafic qui le traverse et ne protège en rien des attaques internes, notamment sur le LAN.

7. Politiques de filtrage

- Selon les besoins, on placera les politiques de filtrage à différents endroits du réseau, au minimum sur chaque hôte contrôlé (pare-feu local) et en bordure du réseau administré sur le pare-feu. Ces emplacements peuvent être distribué dans la topologie selon sa complexité.
- Pour éviter qu'il ne devienne un point unique de rupture, on s'efforcera d'assurer la redondance des pare-feu. On placera plusieurs pare-feu dans l'architecture du réseau à des fins de contrôle au plus proche d'une zone ou pour répartir la charge.

8. Filtrage

- La configuration d'un pare-feu consiste la plupart du temps en un ensemble de règles qui déterminent une action de rejet ou d'autorisation du trafic qui passe les interfaces du pare-feu en fonction de certains critères tels que :

- l'origine et la destination du trafic,
- des informations d'un protocole de couche 3 (IPv4, IPv6, ARP, etc.),
- des informations d'un protocole de couche 4 (ICMP, TCP, UDP, ESP, AH, etc.)
- et/ou des informations d'un protocole applicatif (HTTP, SMTP, DNS, etc.).

9. Décision de filtrage

- Les règles sont appliquées en fonction de la direction du trafic entrant ou sortant sur une interface, avant ou après le processus de routage des paquets. Cette dernière réalité diffère selon le logiciel ou le matériel choisi pour remplir ces tâches.
- Ici l'exemple de la table filter de Netfilter :

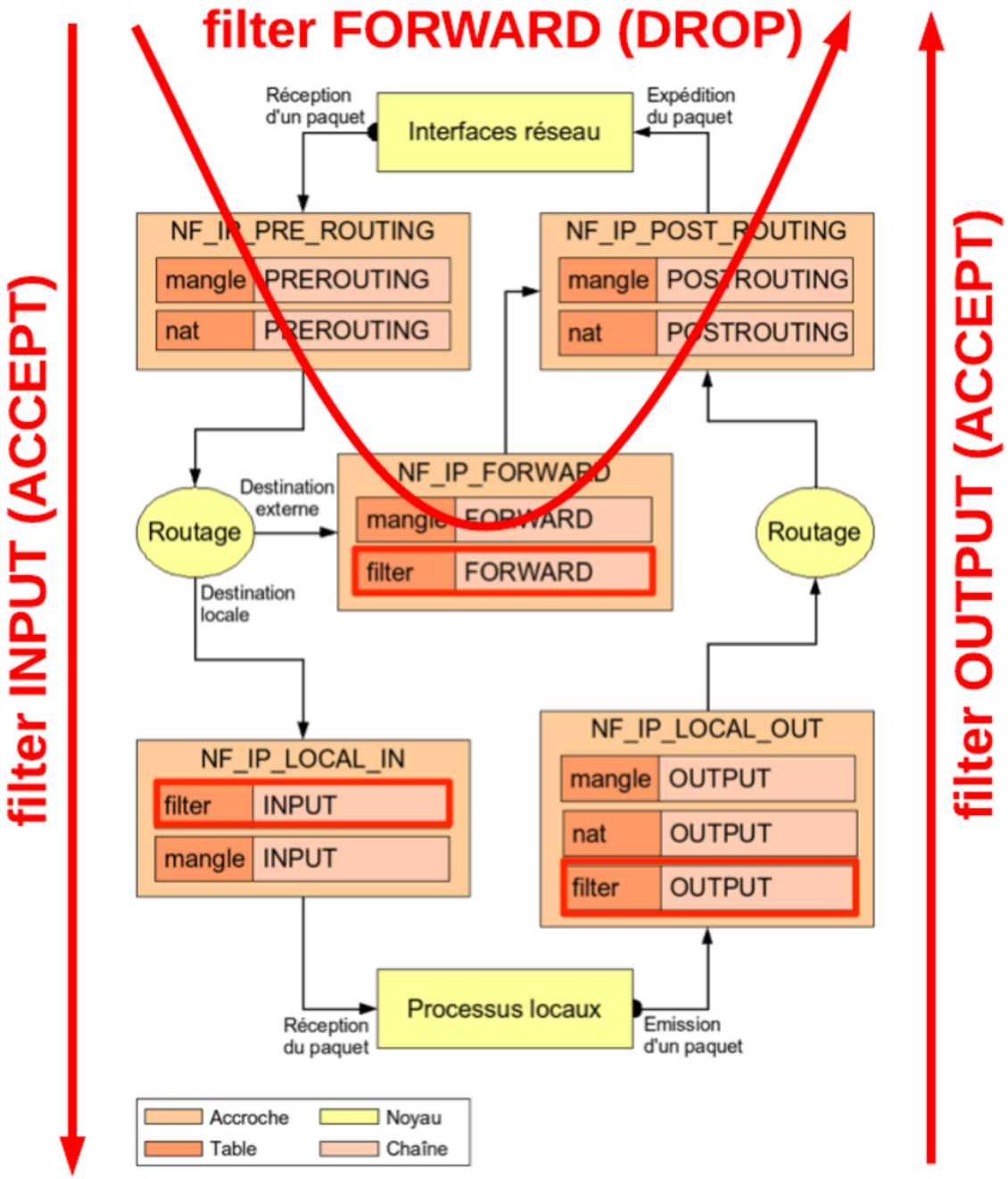


Table filter avec ses chaînes et leur politique par défaut

filter table

10. Règles

- Chaque règle est examinée selon son ordonnancement.
- Si le trafic ne correspond pas à la première règle, la seconde règle est évaluée et ainsi de suite.
- Lorsqu'il y a correspondance entre les critères de la règle et le trafic, l'action définie est exécutée et les règles suivantes ne sont pas examinées.

- La terminologie des actions usuelles peuvent être accept, permit, deny, block, reject, drop, ou similaires.
- En général, un ensemble de règles se termine par le refus de tout trafic, soit en dernier recours le refus du trafic qui traverse le pare-feu. Ce comportement habituellement défini par défaut ou de manière implicite refuse tout trafic pour lequel il n'y avait pas de correspondance dans les règles précédentes.

11. Politique de filtrage typique

On peut résumer des politiques de filtrage typique.

- LAN > WAN
- WAN X LAN
- LAN > DMZ
- DMZ X LAN
- WAN X DMZ (sauf TCP80 par exemple)
- DMZ > WAN

12. Marché des pare-feux NGFW

Le pare-feu est devenu une fonction du réseau qui trouve sa réalité dans les logiciels intégrés aux systèmes d'exploitation des hôtes terminaux, dans les routeurs.

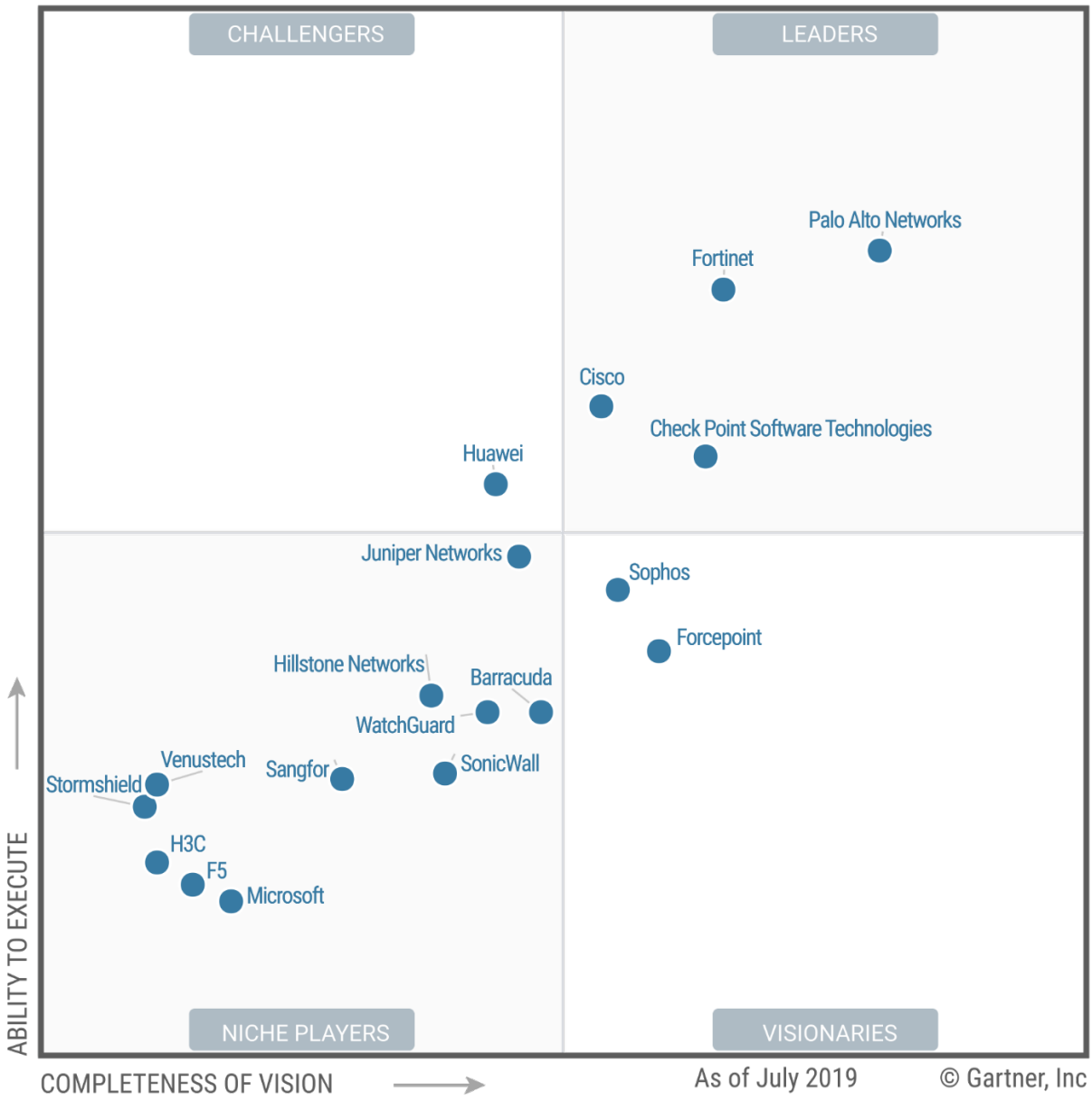
Le successeur embarqué du pare-feu matériel et logiciel est le "next-generation firewall (NGFW)" qui est le pare-feu de troisième génération (le pare-feu sans état étant de la première génération et le pare-feu à état étant de la seconde génération).

Un "next-generation firewall (NGFW)" combine des fonctions traditionneles de pare-feu réseau (NAT, Stateful Inspection et VPN) avec des fonctions avancées de filtrage :

- application firewall using in-line deep packet inspection (DPI)
- intrusion prevention system (IPS)
- TLS/SSL encrypted traffic inspection
- DNS Inspection/Protection
- QoS/bandwidth management
- antivirus inspection
- third-party identity management integration
- SD-WAN features
- Web proxy and content filtering
- Email filtering
- Data loss prevention (DLP)
- Security information and event management (SIEM)

- L2 Filtering
- Virtualization, Virtual Security Domains

12.1. Magic Quadrant for Enterprise Network Firewalls 2019



Magic Quadrant for Enterprise Network Firewalls 2019

12.2. Planning stratégique 2019

- By 2024, 20% of new distributed branch office firewall deployments will switch to **firewall as a service**, up from less than 5% today.
- By 2024, 25% of new firewall deployments will have users consider **cloud-native** firewall policy support of **infrastructure as a service (IaaS) platforms** as a mandatory selection criterion, from less than 5% today.
- By 2024, 50% of new firewall purchases in distributed enterprises will utilize **SD-WAN** features with growing adoption of **cloud-based services**, up from less than 20% today.

12.3. Définition du marché Enterprise Network Firewalls

Le marché des pare-feu réseau représenté par le Magic Quadrant 2019[1] est principalement composé de pare-feu offrant des contrôles bidirectionnels (à la fois en sortie et en entrée) pour sécuriser les réseaux. Ces réseaux peuvent être sur site, hybrides (sur site et dans le nuage), publics ou privés. Les pare-feu réseau peuvent également offrir des fonctionnalités supplémentaires telles que le contrôle des applications, la détection et la prévention des intrusions, la détection avancée des logiciels malveillants, la journalisation et le reporting. Les entreprises qui desservent ce marché se concentrent sur les pare-feu réseau, comme en témoigne la proportion de leurs ventes et de leurs prestations avec leur support, leurs équipes de vente et leurs canaux. Ces vendeurs proposent des fonctionnalités destinées à répondre aux exigences des pare-feu et à résoudre les cas d'utilisation liés aux pare-feu.

Les types de pare-feu réseau envisagés sont les suivants :

- Appliances physiques spécialisés
- Appliances virtuels
- Modules de pare-feu intégré
- Contrôles pare-feu fournis par les fournisseurs de plateformes IaaS

12.4. Planning Stratégique de 2017

> Virtualized versions of enterprise network firewalls will reach 10% of market revenue by year-end 2020, up from less than 5% today.
>
> By year-end 2020, 25% of new firewalls sold will include integration with a cloud-based cloud access security broker (CASB), primarily connected through APIs.
>
> By 2020, 50% of new enterprise firewalls deployed will be used for outbound TLS inspection, up from less than 10% today.

12.5. Magic Quadrant for Enterprise Network Firewalls 2017

Magic Quadrant for Enterprise Network Firewalls 2017

Source : Magic Quadrant for Enterprise Network Firewalls 2017

12.6. Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls) 2017

> Gartner defines the unified threat management (UTM) market as multifunction network security products used by small or midsize businesses (SMBs). Typically, midsize businesses have 100 to 1,000 employees. UTM vendors continually add new functions on the UTM platforms, and therefore they encompass the feature set of many other network security solutions, including, but not limited to :
>
> - Enterprise firewall
> - Intrusion prevention systems (IPSs)
> - Remote access

1. Magic Quadrant for Network Firewalls Published 17 September 2019 - ID G00375686

- Routing and WAN connectivity
- Secure web gateway
- Secure email gateway

Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls) 2017

Source : Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls) 2017

Sixième partie Tunnels VPN IPSEC

Cette partie sur les tunnels VPN IPSEC expose les grands principes du Framework IPSEC de l'IETF. Ensuite, on propose un exercice en Cisco IOS de configuration d'un tunnel IPSEC site à site en mode tunnel auquel on ajoutera un pare-feu. Enfin, on proposera un second exercice en Cisco IOS de configuration d'un tunnel IPSEC entre deux sites en mode transport avec une encapsulation GRE, le tout bien sûr intégré au pare-feu.

6. Framework IPSEC

IPSEC est un standard ouvert de l'IETF pour sécuriser les réseaux IP. Il protège et authentifie les paquets IP d'un origine à une destination grâce à des services de sécurité cryptographiques et à un ensemble de protocoles de transport. IPSEC est un plutôt un "Framework", un cadre évolutif qui ne définit pas des protocoles spécifiques mais des possibilités de sécuriser le transport des données à travers les réseaux IPv4 et IPv6 sous-entendus publics.

1. Services de sécurité

Il assure les fonctions de sécurité suivantes :

Service	Description	Méthode
Confidentilité des données	Des algorithmes de chiffrement confidentialisent le trafic	DES, 3DES, AES
Intégrité des données	Empêche les attaques d'homme-du-milieu et s'assure que les données n'ont pas été modifiée lors de leur transport	HMAC : MD5 ou SHA
Authentification de l'origine	Vérifie l'identité des pairs par un mécanisme d'authentification	PSK, certificats ou nonces RSA, signatures ECDSA
Protection anti-rejeu	-	-
Gestion des clés secrètes	Algorithme de chiffrement asymétrique	Diffie-Hellman (DH) ou ECDH

2. Cadre de sécurité pour IP

IPSEC est un framework, un cadre, qui offre de nombreuses combinaisons protocolaires dans les fonctions citées. Aussi, il n'est pas un protocole en soit, mais plutôt de une combinaison d'entre eux avec des méthodes cryptographiques. La nature de ses composants peut évoluer en fonction des usages et du moment. Il vient compléter les protocoles IPv4 et IPv6 avec des fonctions de sécurité.

3. Protocoles de transport sécurisés

IPSEC propose deux protocoles de couche 3 pour encapsuler le trafic de manière sécurisée : **AH (Authentication Header, IP51)** et **ESP (Encapsulating Security Payload, IP50)**.

3.1. AH (Authentication Header, IP51)

AH (Authentication Header, IP51) est le protocole de transport de la pile IPSEC (RFC 4302) qui assure l'intégrité, l'authentification et une protection anti-rejeu des données échangées. AH signe les paquets IP pour s'assurer que ceux-ci n'ont pas été modifiés lors de leur transport. Alors que L'Internet IPv4 est encore dominant aujourd'hui, AH ne supporte pas les routeurs NAT et le chiffrement de telle sorte qu'il peu déployé dans les réseaux d'entreprise.

3.2. ESP (Encapsulating Security Payload, IP50)

ESP (Encapsulating Security Payload, IP50) est le protocole de transport de la pile IPSEC qui est utilisé pour la confidentialité, l'authentification et l'anti-rejeu des échanges entre deux noeuds IP. ESP protège la charge initiale de couche 3 (qui comprend ou non l'en-tête IP) en le rendant illisible des tiers et en y ajoutant des nouveaux en-têtes dans le réseau public. ESP supporte les routeurs NAT et assure le chiffrement.

4. Modes de fonctionnement IPSEC

Authentication Header (AH) comme Encapsulating Security Payload (ESP) connaissent deux modes de fonctionnement :

- le mode transport
- le mode tunnel.

4.1. IPSEC Mode transport

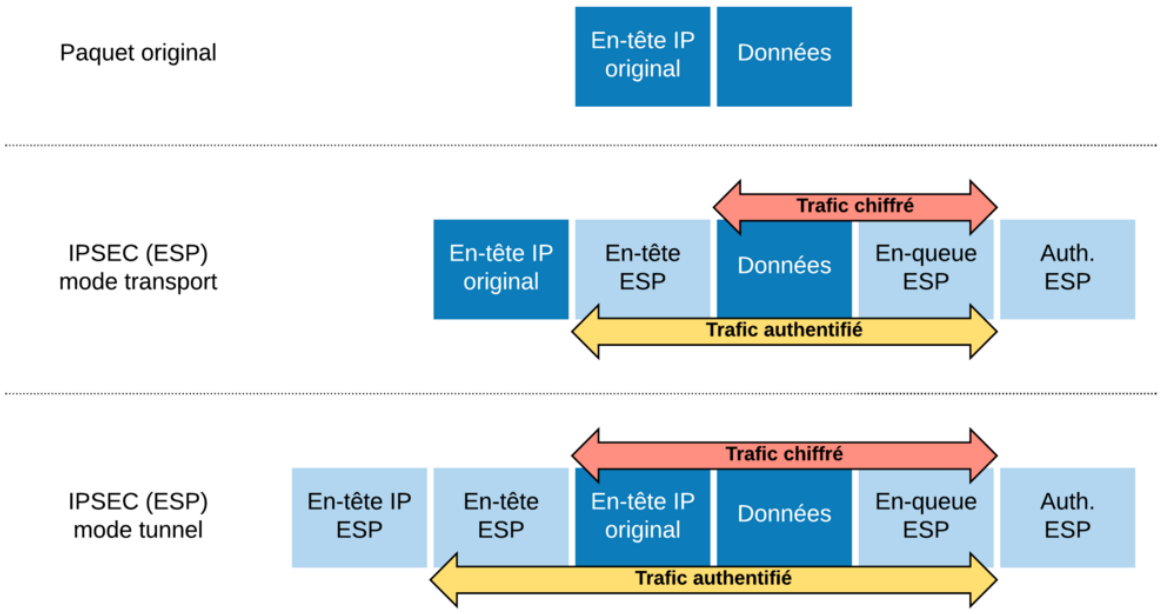
Le mode transport protège uniquement la charge IP. Ce mode ne supporte pas les fonctions de réseaux “overlay” et routage des paquets sur base des en-têtes originaux.

4.2. IPSEC Mode tunnel

Le mode tunnel protège le paquet IP, sa charge et son en-tête original, et IPSEC ajoute des nouveaux en-têtes pour le transport ce qui autorise des fonctions d’overlay et de routage.

4.3. Comparaison des modes transport et tunnel en IPSEC ESP

Dans le diagramme suivant, le paquet original est entitèrement sécurisé (confidentiel et authentifié) en mode tunnel avec un nouvel en-tête IP.



IPSEC ESP en mode transport et en mode tunnel

5. Cryptographie

IPSEC supporte différentes méthodes pour le chiffrement, l’authentification et la gestion des clés.

5.1. Chiffrement symétrique

- DES (56 bits) et 3DES sont dépréciés
- **AES 128, 192 et 256**

5.2. Authentification HMAC

La fonction HMAC est assurée par des protocoles de chiffrement asymétriques :

- md5 Message Digest 5
- sha Secure Hash Standard
- **sha256** Secure Hash Standard 2 (256 bit)
- **sha384** Secure Hash Standard 2 (384 bit)
- **sha512** Secure Hash Standard 2 (512 bit)

5.3. Authentification des pairs

L'authentification des pairs est assurée par IKE grâce à différentes méthodes :

- PSK
- certificats RSA
- nonces RSA
- signatures ECDSA

5.4. Protection des clés

Un protcole asymétrique d'échange de clé comme Diffie-Hellman (DH) de décider d'une clé secrète de chiffriment symétrique dans un environnement de communication non sécurisé. Un groupe Diffie-Hellman (DH) fait référence à la longueur de la clé pour l'échange de clé. Il est recommandé d'implémenter les groupes Diffie-Hellman (DH) 14 et supérieurs.

- 1 Diffie-Hellman group 1 (768 bit)
- 2 Diffie-Hellman group 2 (1024 bit)
- 5 Diffie-Hellman group 5 (1536 bit)
- 14 Diffie-Hellman group 14 (2048 bit)
- 15 Diffie-Hellman group 15 (3072 bit)
- 16 Diffie-Hellman group 16 (4096 bit)
- 19 Diffie-Hellman group 19 (256 bit ecp)
- 20 Diffie-Hellman group 20 (384 bit ecp)
- 21 Diffie-Hellman group 21 (521 bit ecp)
- 24 Diffie-Hellman group 24 (2048 bit, 256 bit subgroup)

6. Transform Sets

Un “Transform set” est une combinaison de protocoles et d’algorithmes de sécurité que les pairs agréent durant la phase de négociation des SA. Dès qu’une correpondance est trouvée, celle-ci est choisie pour sécuriser le trafic AH ou ESP.

6.1. Transform Sets AH

- ah-md5-hmac
- ah-sha-hmac
- ah-sha256-hmac
- ah-sha384-hmac
- ah-sha512-hmac

6.2. Transform Sets ESP de chiffrement

- esp-aes
- esp-gcm
- esp-gmac
- **esp-aes 192**
- **esp-aes 256**
- esp-des
- esp-3des
- esp-null
- esp-seal

6.3. Transform Sets ESP d’authentification

- esp-md5-hmac
- esp-sha-hmac
- **esp-sha256-hmac**
- **esp-sha384-hmac**
- **esp-sha512-hmac**

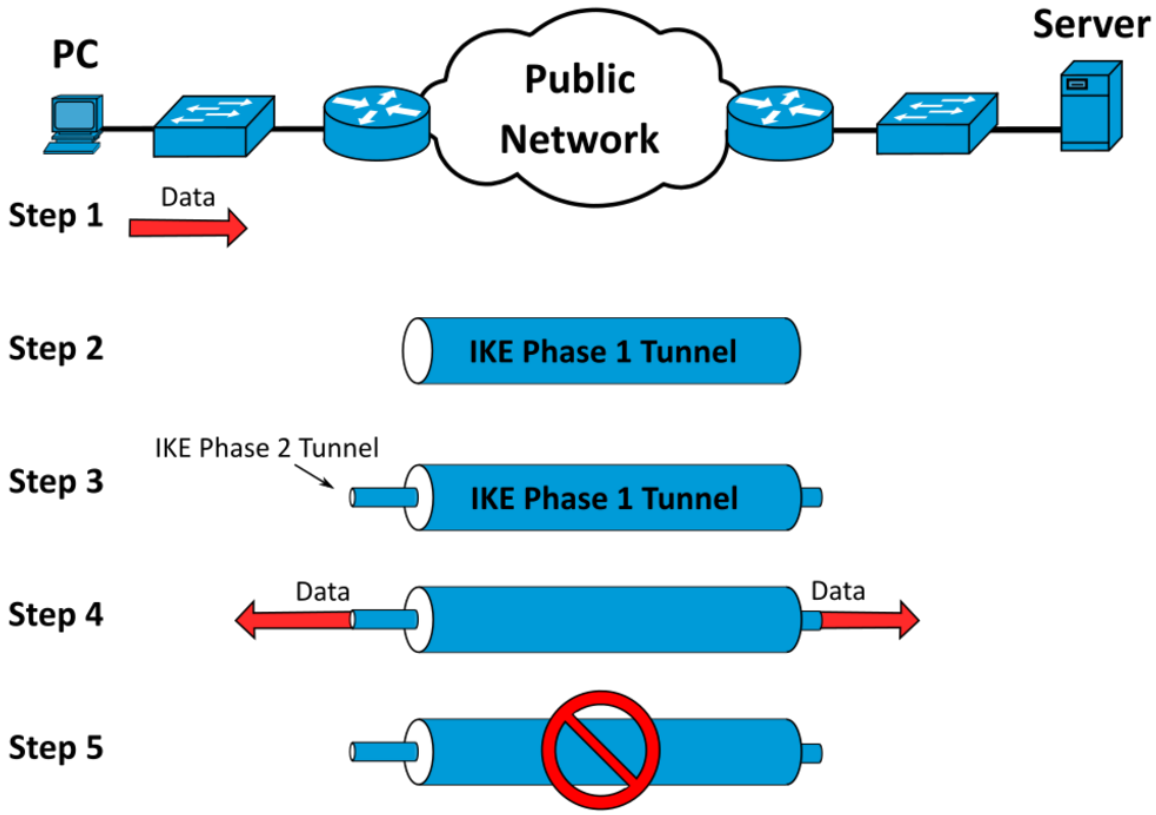
7. Etablissement d’une connexion IPsec

Lors de l’établissement d’une connexion IPsec, plusieurs opérations sont effectuées :

- Etape 1 : Echange des clés

  - IKE phase 1
  - IKE phase 2

- Etape 2 : Transfert de données ESP (ou AH)



Cycle d'un tunnel IPSEC

La première phase d'échange de clés peut être exécutée manuellement mais le protocole IKE (Internet Key Exchange) en version 1 ou en version 2 réalise une authentification pour établir une association de sécurité IPSEC (SA). Ce canal d'échange IKE est réalisé depuis et vers le port UDP 500 ISAKMP (Internet Security Association and Key Management Protocol).

7.1. IKEv1

IKEv1 définit deux phases dans la négociation de clés IKE et l'établissement d'une association de sécurité (SA).

La phase 1 établit une SA bidirectionnelle entre deux pairs IKE (ISAKMP SA). Elle existe en deux modes : main mode (en 6 messages) et aggressive mode (en 3 messages).

Durant cette première phase, des propositions de SA comportent les paramètres suivants et doivent correspondre sur chaque pair :

- Algorithme de hash : MD5 (déprécié) ou SHA.
- Algorithme de chiffrement : DES, 3DES (dépréciés) ou AES.
- Méthode d'authentification : PSK (Pre-Shared Key) ou certificats numériques.
- Groupe Diffie-Hellman (DH) : Group 1, 2, 5 (dépriciés) et ainsi de suite.

- Temps de vie (SA Lifetime) : Durée de vie du tunnel (par défaut 24 heures). C'est le seul paramètre qui peut être différent d'un pair à l'autre (en cas de différence, c'est la valeur la plus faible qui est choisie).

La phase 2 établit en 3 messages des SAs unidirectionnels bénéficant des ISAKMP SA établis lors de la phase 1.

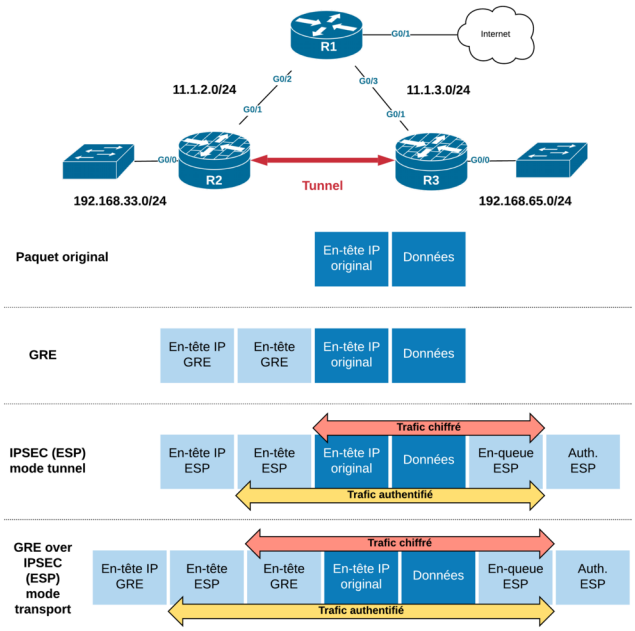
7.2. IKEv2

IKEv2 est l'évolution d'IKEv1 avec les carctéristiques suivantes :

- 4 messages plus efficients
- Supporte des méthodes d'authentification EAP
- Supporte des méthodes cryptographiques récentes

8. Solution VPN IPSEC et GRE over IPSEC

On trouve plusieurs types de déploiement de VPN IPSEC. Le seul véritablement inter-opérable est le modèle de tunnel Site-à-Site. On ira utilement relire la définition et les typologies de VPN.



Lab IPSEC ESP en mode tunnel et en mode transport avec GRE intégré au pare-feu ZBF

En mode "tunnel" entre deux sites, le paquet IP original est entièrement chiffré et un nouvel en-tête IP est fabriqué par IPSEC avec les adresses publiques des deux points en source et en destination.

Avec GRE, en mode "transport" ESP ne chiffre que la charge sans ajouter de nouvel en-tête IP. Mais quelle sera l'en-tête IP original non chiffré ? Celui que le tunnel GRE aura créé. Quelle sera la charge chiffrée ? Celle du tunnel GRE qui comprendra l'en-tête GRE et le paquet IP original. Cette configuration autorise le trafic multicast dans le tunnel.

On trouvera touefois d'autres implémentations des tunnels IPSEC qui supportent des fonctionnalités avancées comme DMVPN, FlexVPN ou des solutions propriétaires sur les gammes de pare-feu NG.

9. Configuration de tunnels VPN en Cisco IOS

Deux méthodes de configuration :

- par Crypto-map
- par profils de tunnel IPSEC sur interface tunnel GRE

9.1. Configuration par Crypto-map

1. Créer un crypto-acl qui identifie le trafic du tunnel.
2. Créer une ISAKMP policy pour la IKE SA.
3. Configurer une clé partagée pour l'authentification ISAKMP.
4. Créer un Transform Set qui indique le mode et les protocoles AH et ESP.
5. Créer un Crypto-map qui indique la crypto-acl, l'adresse du pair et le Transform Set à utiliser.
6. On applique le Crypto-map sur l'interafce externe.

9.2. Configuration par profils de tunnel IPSEC

1. Créer une ISAKMP policy pour la IKE SA.
2. Configurer une clé partagée pour l'authentification ISAKMP.
3. Créer un Transform Set qui indique le mode et les protocoles AH et ESP.
4. Créer un profil de tunnel IPSEC qui indique le Transform Set.
5. Appliquer le profil de tunnel IPSEC sur l'interface du tunnel (commande `tunnel protection ipsec profile ...`)

9.3. Valeur par défaut

- Algorithme de chiffrement : DES (56 bits)
- Algorithme de hash : SHA1
- Méthode d'authentication : RSA Signature
- Groupe Diffie-Hellman : `#1`
- SA lifetime : 86400 seconds

9.4. Configuration Pare-feu

- ISKAMP : UDP 500
- ESP : IP 50
- AH : IP 51
- GRE : IP 47

9.5. Configuration NAT

Le trafic entre les réseaux privés ne devrait pas être traduit.

Septième partie Examen CCNA 200-301

...

7. Diagnostic fondamental sur les hôtes terminaux

On trouvera dans ce document une synthèse des méthodes de dépannage sur les hôtes terminaux qui consiste à éprouver les trois paramètres d'une connectivité TCP/IP bien vécue : une adresse IP et son masque, une passerelle par défaut et un serveur de résolution de noms.

1. Interaction des protocoles

- Avant qu'une interface puisse envoyer du trafic faut-il :
- qu'elle ait obtenu une adresse IP statique ou dynamique (DHCP en IPv4 ou autoconfiguration/DHCPv6 en IPv6) ;
- qu'elle ait résolu le nom de l'hôte destinataire en adresse IP (DNS sur IPv4 ou sur IPv6) ;
- qu'elle ait obtenu l'adresse de livraison physique de la destination locale ou de la passerelle par défaut si la destination n'est pas locale (ARP en IPv4 ou ND en IPv6).

2. Autres protocoles de gestion

- D'autres protocoles de gestion importants se rencontreront dans les réseaux TCP/IP, à titre d'exemples :
- ICMP qui permet en IPv4 et en IPv6 d'obtenir du diagnostic IP (`ping` et `traceroute`).
- NTP qui permet de synchroniser les horloges des hôtes sur le réseau.
- SNMP qui permet de collecter des informations sur le matériel à travers le réseau.
- SSH qui permet de monter une console distante à travers TCP/IP.
- Le routage IP met en oeuvre du NAT sur les passerelles des réseaux privés pour offrir une connectivité à l'Internet.
- …

3. Paramètres TCP/IP

Il y a trois paramètres nécessaires pour établir une connexion TCP/IP globale à partir d'une ordinateur :

- Une adresse IP et son masque
- Une passerelle par défaut
- Un serveur de résolution de noms

3.1. Une adresse IP et son masque

Vérification des interfaces

Sous Linux :

- `ip addr show`
- `ifconfig`

Sous Windows :

- `ipconfig`
- `netsh interface ipv4 show add`
- `netsh interface ipv6 show add`

Test de connectivité IP

Sous Windows en IPv4 sans connectivité IPv6

- `ping www.test.tf`

Sous Linux en IPv4 (ping) et en IPv6 ping6

- `ping www.test.tf`
- `ping6 www.test.tf`

3.2. Passerelle par défaut

Vérification de la table de routage (IPv4/IPv6)

Sous Linux :

- `ip route`

Sous Windows :

- `ipconfig`
- `route`
- `netsh interface ipv4 show route`
- `netsh interface ipv6 show route`

Vérification des sauts

Sous Windows :

- `tracert 176.31.61.170`

Sous Linux :

- `traceroute 176.31.61.170`

3.3. Serveur de nom

Sous Linux :

- `cat /etc/resolv.conf`

Sous Windows :

- `ipconfig /all`
- `netsh interface ipv4 show ?`
- `netsh interface ipv6 show ?`

Requêtes DNS

Sous Linux

- `nslookup`
- `dig`

Sous Windows

- `nslookup`

4. ping

Ping est une commande système qui vérifie la connectivité d'une destination avec ICMP. Elle génère du trafic identifiable : des paquets "ICMP echo request" (type 8, code 0) en vue de vérifier la connectivité.

La commande attend des paquets ICMP de retour : au mieux des "ICMP Echo Reply" (type 0, code 0). Si d'autres messages sont reçus (Destination Unreachable, TTL exceeded, …) ces derniers sont affichés.

En origine , les paquets ICMP prennent l'adresse IP de l'interface la plus proche de la destination.

4.1. ping : vérification

- Détermine trois éléments :
- Si une interface IP est active ou pas par ICMP
- Le délai des paquets
- Le taux de perte des paquets
- Ici la réception de quatre echo reply :

```
$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=9.31 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=9.41 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=9.34 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=9.41 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 9.317/9.371/9.417/0.080 ms
```

4.2. ping : interprétation

- Le diagnostic s'arrête à ICMP et monte à la couche L7 en tentant de joindre des noms.
- L'hôte de destination peut être configuré pour ne pas répondre à ces requêtes (pare-feu configuré traditionnellement)
- Peut signifier un problème de routage dans le chemin (un routeur n'arrive pas à placer le paquet).
- Un élément (pare-feu, proxy) peut filtrer ce trafic dans le chemin.
- Les résultats de délais et de perte permettent de qualifier la qualité de la transmission. C'est utile pour diagnostiquer du trafic d'applications en temps réel (VoIP, streaming, jeux en ligne, ...).

4.3. Connectivité IP globale

- Vérification de la connectivité locale : vers la passerelle
- Vérification de la connectivité globale vers une adresse IP globale bien connue :
- En Belgique, les serveurs DNS de Belgacom : `195.238.2.21`, `195.238.2.22`
- Les serveurs DNS IPv4 de Google : `8.8.8.8`, `8.8.4.4`

4.4. ping 8.8.8.8

- Quel est le trafic généré par un `ping 8.8.8.8` ?

```
aa:bb:cc:dd:ee:ff > ff:ff:ff:ff:ff:ff, ARP, length 42: Request who-has 10.185.220.95 tell 10.185.220.1\
33, length 28
c8:d7:19:23:b6:bf > aa:bb:cc:dd:ee:ff, ARP, length 60: Reply 10.185.220.95 is-at c8:d7:19:23:b6:bf, le\
ngth 46
aa:bb:cc:dd:ee:ff > c8:d7:19:23:b6:bf, IPv4, length 98: 10.185.220.133 > 8.8.8.8: ICMP echo request, i\
d 14174, seq 1, length 64
c8:d7:19:23:b6:bf > aa:bb:cc:dd:ee:ff, IPv4, length 98: 8.8.8.8 > 10.185.220.133: ICMP echo reply, id \
14174, seq 1, length 64
```

5. traceroute/tracert

Les commandes `traceroute` et `tracert` (Windows) permettent de détecter les routeurs entre la station d'origine et une destination.

- tracert complet sous Windows à destination de 8.8.8.8
- tracert sous Linux à destination de 8.8.8.8 (quatrième saut).

5.1. Tracert (Windows)

- Le logiciel envoie trois messages ICMP echo request (type 8, code 0) avec un TTL de 1, puis de 2, et ainsi de suite.
- Trois réponses sont attendues de la passerelle qui filtre le TTL à 1 : des messages ICMP “TTL Exceeded in Transit” avec des identifiers et Sequence Numbers correspondants.

5.2. traceroute (Linux)

- Le logiciel envoie trois messages UDP avec un TTL de 1, puis de 2, et ainsi de suite. Chaque message est à destination d’un port UDP différent.
- Trois réponses sont attendues de la passerelle intermédiaire qui filtre le TTL à 1 : des messages ICMP “TTL Exceeded in Transit” embarquant le message UDP original avec son port de destination. Les trois réponses sont représentées dans les trois délais de la sortie.

5.3. traceroute interprétation

- Délais : Round Trip (RTT)
- Délais : détermine la qualité des liaisons (congestion)
- Délais : mais aussi la distance (propagation)
- Adresses des interfaces d’entrées
- Localisation
- Fournisseur
- A lier avec un whois
- http ://www.nanog.org/meetings/nanog47/presentations/Sunday/RAS_Traceroute_N47_Sun.pdf

5.4. traceroute : exemple

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  WDR3600-D3.lan (192.168.100.1)  3.299 ms  3.518 ms  3.434 ms
 2  88.147.32.1 (88.147.32.1)  27.768 ms  27.690 ms  36.957 ms
 3  88.147.95.13 (88.147.95.13)  36.936 ms  37.300 ms  37.230 ms
 4  ge-2-2-2-193.bru20.ip4.tinet.net (77.67.76.121)  37.154 ms  37.076 ms  37.059 ms
 5  xe-0-0-2.ams60.ip4.tinet.net (89.149.180.121)  42.757 ms  42.678 ms  43.997 ms
 6  as15169.ams60.ip4.tinet.net (141.136.102.246)  64.105 ms  60.201 ms  78.499 ms
 7  209.85.248.92 (209.85.248.92)  59.925 ms 209.85.248.112 (209.85.248.112)  34.158 ms  33.950 ms
 8  72.14.238.69 (72.14.238.69)  40.288 ms 209.85.253.249 (209.85.253.249)  64.905 ms  52.239 ms
 9  209.85.254.231 (209.85.254.231)  58.553 ms  59.042 ms  58.659 ms
10  209.85.255.51 (209.85.255.51)  64.564 ms 209.85.254.189 (209.85.254.189)  58.307 ms 216.239.49.30 \
(216.239.49.30)  58.246 ms
11    * * *
12  google-public-dns-a.google.com (8.8.8.8)  58.556 ms  58.716 ms  43.237 ms
```

6. Vérification de la table de routage

…

7. Vérification de la table de voisinage IPv4/IPv6

…

8. Vérification des ports TCP/UDP

8.1. Commande `netstat`

- `netstat`, pour “network statistics”, est une ligne de commande affichant des informations sur les connexions réseau, les tables de routage et un certain nombre de statistiques dont ceux des interfaces, sans oublier les connexions masquées, les membres Multicast, et enfin, les messages netlink.
- La commande est disponible sous Unix (et ses dérivés dont Linux) et sous Windows NT compatibles.

8.2. Commande `ss`

- Les ports TCP/UDP IPv4/IPv6 à l’écoute :

```
# ss -antp
State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
LISTEN     0      128            *:22                        *:*                   users:(("sshd",pid\
=17454,fd=3))
LISTEN     0      128    127.0.0.1:631                       *:*                   users:(("cupsd",pi\
d=834,fd=13))
LISTEN     0      100    127.0.0.1:25                        *:*                   users:(("master",p\
id=1359,fd=13))
LISTEN     0      128         :::80                      :::*                  users:(("httpd",pid=99\
32,fd=4),("httpd",pid=9931,fd=4),("httpd",pid=9930,fd=4),("httpd",pid=9929,fd=4),("httpd",pid=9928,fd=\
4),("httpd",pid=9925,fd=4))
LISTEN     0      128         :::22                      :::*                  users:(("sshd",pid=174\
54,fd=4))
LISTEN     0      128        ::1:631                     :::*                  users:(("cupsd",pid=83\
4,fd=12))
```

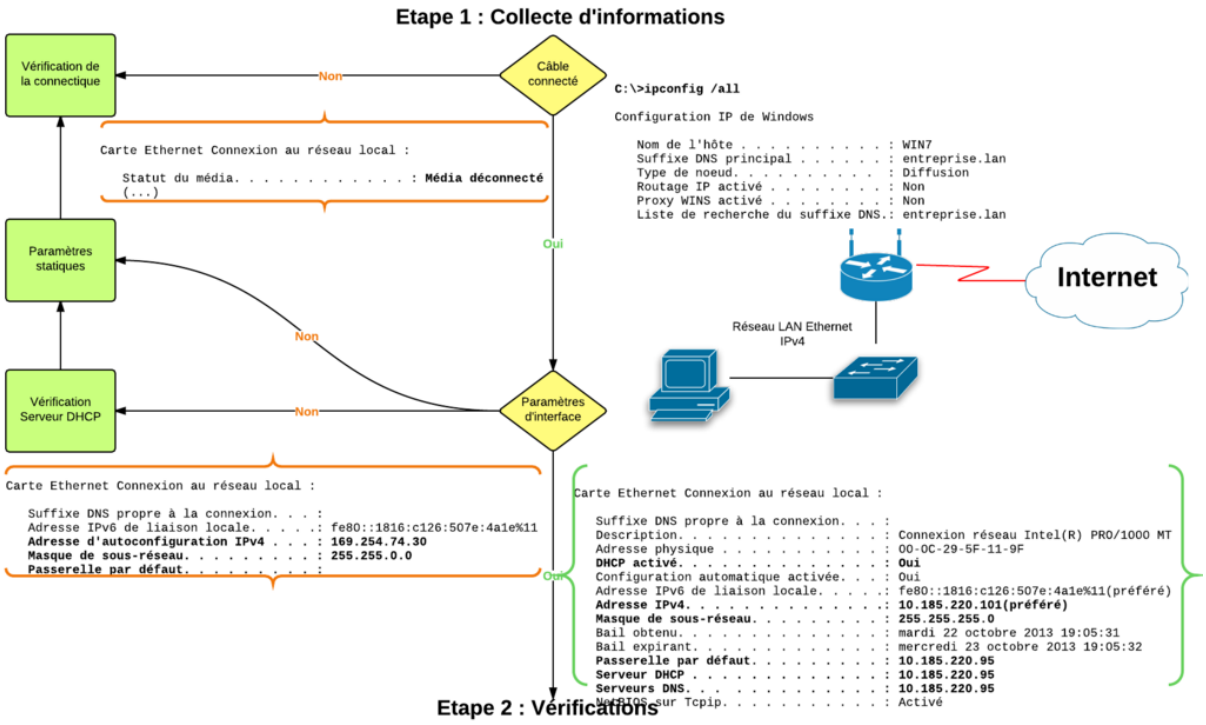
- Toutes les sessions :

```
# ss -a
```

9. Diagnostic fondamental

- 1. Collecte d’information :
- Connexion de l’interface (oui/non)
- Adresse IP, masque, passerelle, serveur DNS, serveur DHCP (paramètres)
- 1. Vérification :
- Résolution de noms
- Connectivité globale
- Connectivité locale
- Routage

9.1. Collecte d'information TCP/IP



Collecte d'information TCP/IP

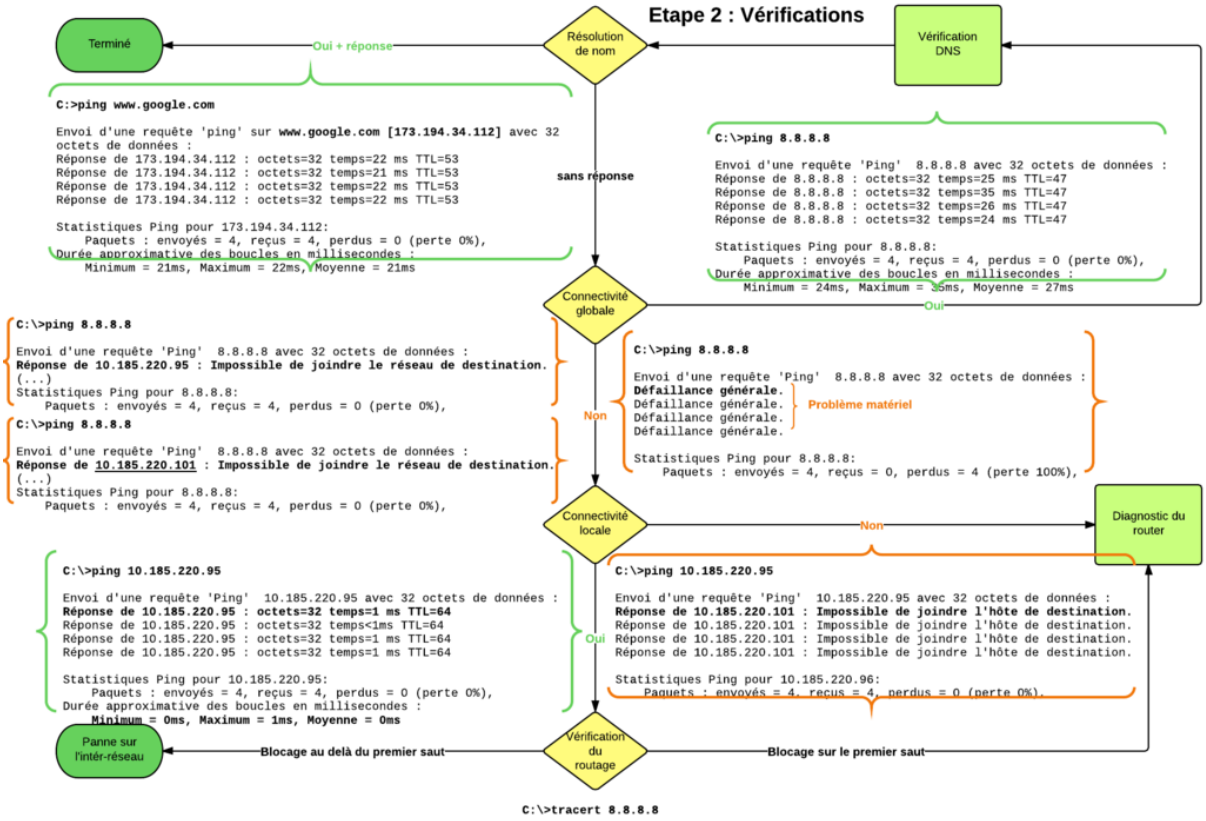
(Sorties type Windows)

- Commandes :

```
$ ip link show
$ ip addr show
```

- Le câble est-il branché ? problème physique/infrastructure
- Y voit-on des paramètres TCP/IP ?
- Comment sont-ils attribués ? Problème de configuration d'interface.

9.2. Vérifications TCP/IP



Vérifications TCP/IP

(Sorties type Windows)

- Résolution de nom : `ping www.google.com`
- `nslookup` / `dig`
- Connectivité globale : `ping 8.8.8.8`
- réponse négative distante
- réponse négative locale
- pas de réponse
- Connectivité locale : `ping [passerelle]`
- Vérification du routage : `ip route show` / `traceroute`

Révisions

Sécurité

- Définir les concepts clé de la sécurité (menaces, vulnerabilités, exploits, et les techniques d'atténuation)
- Décrire les éléments des programmes de sécurité (sensibilisation des utilisateurs, formation, le contrôle d'accès physique)
- Décrire les éléments des politiques de sécurité comme la gestion, la complexité, et les alternatives aux mots de passe (authentications multifacteur, par certificats, et biométriques)
- AAA
- DHCP snooping
- dynamic ARP inspection
- ~~Décrire les protocoles de sécurité sans-fil (WPA, WPA2, et WPA3)~~
- ~~Configurer un WLAN en utilisant WPA2 PSK avec un GUI~~

Automation / Design

- Spine-leaf
- Comparer les réseaux traditionnels avec le réseau basé contrôleur (controller-based)
- Décrire les architectures basées contrôleur (controller-based) et software defined (overlay, underlay, et fabric) : Séparation du control plane et du data plane, APIs North-bound et south-bound
- Comparer la gestion traditionnelle les périphériques campus avec une gestion des périphériques avec Cisco DNA Center