Protection des Applications Critiques et Métiers dans les Réseaux d'Entreprise Multi-Sites

MERISAC
INSTRUMENTS
Intégrateur de Services Datacenter & Cloud

TABLE DES MATIERES

I) INTRODUCTION 3

II) ARCHITECTURE TYPIQUE DES RESEAUX D'ENTREPRISE MULTI-SITES EN FRANCE 4

III) LES APPLICATIONS CRITIQUES ET METIERS 5

1) LES APPLICATIONS CRITIQUES 5

2) LES APPLICATIONS METIERS 6

IV) POURQUOI LES APPLICATIONS CRITIQUES ET METIERS DU RESEAU D'ENTREPRISE MULTI-SITES SONT-ELLES VULNERABLES ? 7

1) CAUSE RESEAU : TOUTES LES APPLICATIONS DU RESEAU SE PARTAGENT LA MËME BANDE PASSANTE 7

2) CAUSE SECURITE : ATTAQUES DE DENI DE SERVICE SUR LE RESEAU D'ENTREPRISE ET LES SERVEURS 9

V) IDENTIFICATIONS DES GROUPES D'APPLICATIONS RISQUANT DE PERTURBER LES APPLICATIONS CRITIQUES ET METIERS 10

VI) ETUDE DES FAUSSES BONNES SOLUTIONS CENSEES PROTEGER LES APPLICATIONS CRITIQUES ET METIERS 11

1) CONTRÔLE DU TRAFIC APPLICATIF PAR ROUTEUR 11

2) CONTRÔLE DU TRAFIC APPLICATIF PAR FIREWALL 13

3) CONTRÔLE DU TRAFIC APPLICATIF PAR SD-WAN 14

VII) SOLUTIONS EFFICACES POUR PROTEGER LES APPLICATIONS CRITIQUES ET METIERS A PARTIR D'UN CONTRÔLEUR DE QoS 15

1) DEPLOIEMENT TYPIQUE D'UNE SOLUTION ALLOT DANS UN RESEAU D'ENTREPRISE MULTI-SITES 15

2) VISIBILITE TRADITIONNELLE SUR LES FLUX APPLICATIFS 16

3) VISIBILITE ANALYTIQUE SUR LES FLUX APPLICATIFS 17

4) CONTRÔLE DE QOS SUR LES FLUX APPLICATIFS 19

5) PROTECTION ANTI-DDOS AVEC MITIGATION DES CYBERATTAQUES 22

6) TEMOIGNAGES CLIENTS 24

VIII) CONCLUSION 25

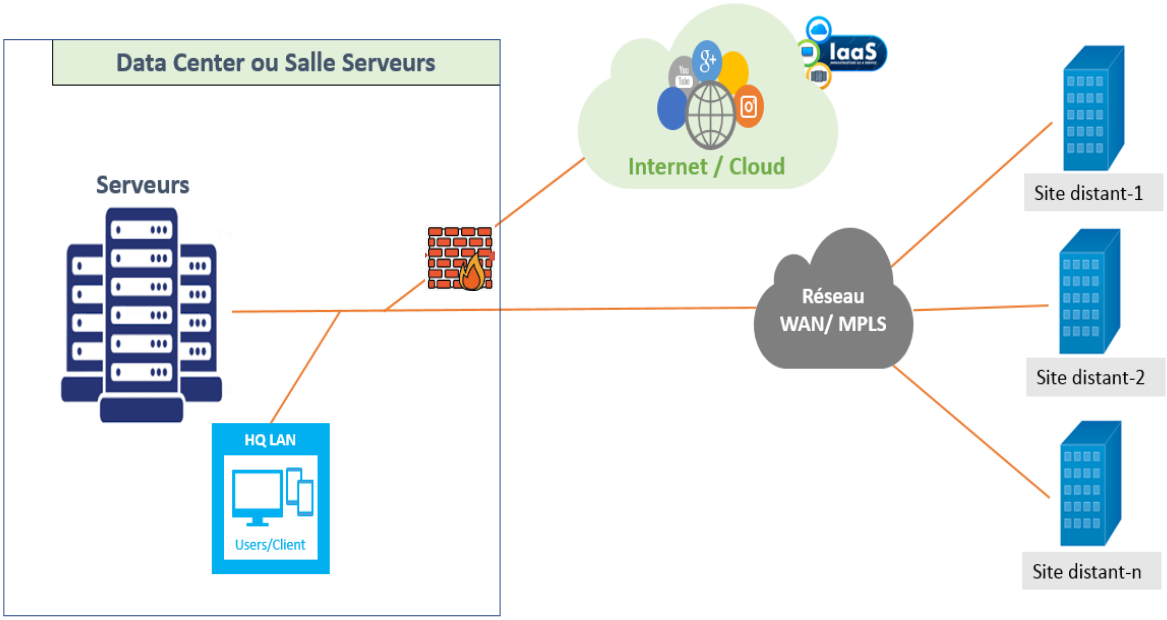
I) INTRODUCTION

Les applications critiques et métiers jouent un rôle vital dans le fonctionnement des entreprises. Cependant, la coexistence de multiples applications sur le réseau d'entreprise peut entraîner des défis de performance pour ces applications essentielles. Ce livre blanc examine en profondeur, d'une part, les risques de dégradation des performances engendrés par la concurrence entre applications circulant sur le réseau d'entreprise multi-sites et, d'autre part, les cybermenaces liées aux attaques de déni de service. Ce livre blanc propose des solutions pour y remédier dans le but d'assurer une qualité d'expérience optimale aux utilisateurs de l'entreprise et d'éliminer les interruptions de service intempestives, plus ou moins longues, qui affectent très négativement la productivité de l'entreprise.

Heureusement, la plupart des services informatiques sont sensibilisés à une protection de tous les instants de ces applications critiques et métiers pour garantir la confidentialité, l'intégrité et la disponibilité des données de l'entreprise. Cette prise de conscience est d'autant plus importante, qu'en abordant cette 3ème décennie, la complexité et l'hétérogénéité du réseau d'entreprise s'est considérablement accrue en raison de l'évolution rapide de la technologie. Pour s'en convaincre, il suffit de constater la multitude de technologies nouvelles qui vont du Cloud Computing à l'Internet des Objets (IoT), en passant par l'Intelligence Artificielle, le SD-WAN et la 5G,…. En outre, les employés utilisent une grande variété de dispositifs pour se connecter au réseau de l'entreprise et à Internet (ordinateurs, smartphones, tablettes, …), sur place ou en télétravail, et de plus en plus d'applications sont hébergées de manière hybride dans un datacenter, une salle serveur ou le cloud.

Tous ces élements donnent du fil à retordre, en premier lieu, aux responsables d'infrastructure réseau et, par ricochet, aux responsables des services informatiques dont le « help desk » court le risque d'être submergé par les plaintes de leurs utilisateurs liées aux baisses de performance de leurs applications critiques ou métiers. Dans ce contexte, les DSI et les Responsables Informatiques n'ont d'autre choix que de s'équiper de solutions efficaces capables d'assurer la visibilité et le contrôle de l'ensemble des applications. A ce défi de taille, ajoutons celui des cybermenaces qui constituent une épée de Damocles permanente sur la tête de ces responsables du fait de la nature polyforme des cyberattaques (DDoS). Contre ces dernières, des mesures par anticipation strictes doivent aussi être prises quelle que soit la taille de l'entreprise afin d'éviter un effondrement toujours possible du réseau d'entreprise. Par ailleurs, les solutions retenues doivent être protégées contre les éventuelles éventuelles vulnérabilités des systèmes qui, lorsqu'elles sont exploitées, risquent de se transformer en dangereuses failles de sécurité.

II) ARCHITECTURE TYPIQUE DES RESEAUX D'ENTREPRISE MULTI-SITES EN FRANCE



Un réseau d'entreprise multi-sites est une infrastructure appartenant à la même organisation qui relie plusieurs sites physiques géographiquement dispersés au sein d'un réseau interconnecté. Ces sites peuvent être des bureaux, des succursales, des usines, des centres de données (datacenter) ou toute autre installation de l'entreprise. L'objectif du réseau d'entreprise est de permettre une communication fluide entre les différentes entités du réseau (postes de travail, serveurs internes, serveurs Web, …), un partage de données efficace et un accès centralisé aux ressources de l'entreprise (datacenter, salle serveurs ou IaaS).

Les sites distants sont interconnectés à l'aide de divers moyens de communication tels que des lignes dédiées, des liaisons VPN, des connexions Internet sécurisées (SD-WAN) ou des réseaux privés gérés par des opérateurs de réseaux (MPLS). Actuellement, la topologie utilisée par près de 80% des entreprises en France est illustrée dans la figure, ci-dessus. D'une part, les serveurs internes, hébergés dans un datacenter ou une salle serveurs, sont reliés par LAN aux éventuels utilisateurs locaux et aux utilisateurs distants par un réseau WAN ou MPLS. D'autre part, l'accès Internet est centralisé dans le datacenter ou la salle serveurs de manière à assurer une sécurité centralisée vers Internet et le cloud, notamment, grâce aux firewalls et aux sondes IPS (Intrusion Prévention System). Le concept du SD-WAN constitue une autre technique afin que les utilisateurs des sites distants puissent accéder directement à Internet et au cloud, mais il n'a pas encore trouvé les faveurs d'une majorité d'entreprises en France malgré ses 7 ans d'existence. Nous reviendrons brièvement sur le SD-WAN un peu plus tard pour en comprendre les raisons.

III) LES APPLICATIONS CRITIQUES ET METIERS

1) LES APPLICATIONS CRITIQUES

Dans un réseau d'entreprise, les applications critiques varient en fonction du secteur d'activité, de la taille de l'entreprise, de ses besoins propres et de sa stratégie informatique. Cependant, il existe plusieurs catégories d'applications qui sont considérées comme critiques dans la plupart des environnements professionnels. Voici quelques exemples :

* **Applications de Communication et de Collaboration** telles que Microsoft Teams, Zoom, Skype for Business, … qui facilitent la communication en temps réel et la collaboration.

* **Applications de Messagerie Electronique** telles que Microsoft Outlook, Gmail, Lotus Notes, ...

* **Applications de Gestion de Projets** telles que Microsoft Project, Asana, Jira, … pour la planification et le suivi de projets

* **Applications de Gestion de la Relation Client (CRM)** telles que Salesforce, Microsoft Dynamics 365, Hubspot, … qui gèrent les interactions clients, ventes et marketing.

* **Applications de Gestion des Ressources Humaines** telles que SAP, Workday, SuccessFactors, … qui gèrent la paie, les congés, les évaluations humaines et le recrutement.

* **Applications de Virtualisation** telles que VMware, Microsoft Hyper-V, … pour la virtualisation des serveurs, du stockage et du poste de travail, …

* **Applications de Services Cloud** telles que Amazon Web services (AWS), Microsoft Azure, Google Cloud Platform, …pour l'hébergement et l'exécution des applications.

* **Applications de Sécurité** telles que Palo Alto Networks, Cisco Umbrella, …. pour garantir la sécurité du réseau et la gestion des accès.

Ces applications jouent un rôle critique dans le fonctionnement et la gestion des opérations au sein des entreprises. L'optimisation de la bande passante et la garantie des performances doivent être au cœur des préoccupations du responsable d'infrastructure afin d'assurer une productivité optimale et la continuation des activités en toutes circonstances, si possible, par une solution qui automatise le processus de contrôle du trafic applicatif.

2) LES APPLICATIONS METIERS

Les applications métiers qui circulent dans un réseau d'entreprise varient en fonction du secteur d'activités et des besoins spécifiques de l'entreprise. Voici quelques catégories d'applications métiers couramment utilisées :

- ***Finance* - Système de Gestion Financière (SGF)** : applications de comptabilité, de gestion des transactions, de budgétisation et de planification financière, …
- ***Finance* - Plateforme de Trading** : opérations de trading, gestion des investissements et analyse des marchés financiers, …
- ***Santé* - Systèmes d'Information Hospitaliers (SIH)** : applications pour la gestion des dossiers médicaux électroniques, planification des ressources, gestion des rendez-vous et facturation, …
- ***Manufacture et Logistique* - Systèmes de Gestion de la Qualité** : applications pour le contrôle qualité et la conformité aux normes, …
- ***Commerce de Détail et E-Commerce* - Plateformes de Commerce Electronique** : applications pour la gestion des commandes en ligne, traitement des paiements et expérience client, …
- ***Plateforme de Collaboration Educative*** : applications pour la collaboration entre enseignants et élèves, échange de ressources éducatives, …
- ***Services Professionnels - Logiciels de Gestion de Projets*** : applications de planification, budgétisation et suivi de projets
- ***Technologie de L'Information* - Logiciels de Gestion des Services Informatiques (ITSM)** : applications pour gestion des incidents, des changements et des actifs informatiques
- ***Services Publics* - Systèmes de Gestion des Services Publics** : applications pour la gestion des services d'eau, d'électricité et de gaz, …

Chaque secteur utilise ses propres applications métiers en fonction de ses propres processus. Soit ces applications métiers existent sur le marché des logiciels SaaS, après qu'elles aient subi quelques adaptations liées aux besoins spécifiques de chaque entreprise, soit elles font l'objet d'un développement logiciel intégral par une entité interne à l'entreprise ou un prestataire extérieur.

IV) POURQUOI LES APPLICATIONS CRITIQUES ET METIERS DU RESEAU D'ENTREPRISE MULTI-SITES SONT-ELLES VULNERABLES ?

1) CAUSE RESEAU : TOUTES LES APPLICATIONS DU RESEAU SE PARTAGENT LA MËME BANDE PASSANTE

Toutes les applications gourmandes en bande passante sont susceptibles de perturber les applications critiques et métiers, notamment en affectant leur performance, leur disponibilité, leur qualité de service ou leur sécurité. Juste après ce chapitre, nous identifierons les autres applications du réseau potentiellement perturbatrices. Voici plusieurs situations face auxquelles le responsable d'infrastructure doit se montrer particulièrement vigilant :

- **Congestion du réseau**
  - Par définition, toutes les applications empruntent les mêmes tuyaux du réseau, qu'ils soient cuivres ou optiques. Cependant, au niveau du datacenter ou d'une salle serveurs, il y a peu de chance d'atteindre la saturation des liaisons parce qu'elles sont, en principe, dimensionnées très largement pour éviter ce genre de désagrément. D'ailleurs, il est fréquent de trouver des liaisons vers Internet et/ou le WAN à 1 Giga bits/seconde, même pour des entreprises de taille moyenne. En revanche, sur les sites distants, les opérateurs renoncent dans certains cas à proposer des débits de liaisons supérieurs à 10 Mbps car il faudrait engager des travaux de génie civil trop coûteux. Pour ces sites distants, le risque de subir des baisses de performance pour les applications critiques ou métiers est patent. Le problème n'est pas lié au coût des liaisons dont la montée en bande passante est de moins en moins chère, mais d'une impossibilité matérielle pour les opérateurs de les proposer. Par conséquent, il faut trouver une solution pour ces sites distants afin de compenser leur faible débit. Cette solution passe par un contrôle granulaire des flux applicatifs comme nous le verrons plus tard dans le volet des solutions que nous préconisons.

- **Qualité de Service réseau (QoS)**
    - La Qualité de Service du réseau (QoS) est définie par les quatre paramètres suivants : Le Débit ou la bande passante (Mbps), la Latence réseau (ms), la Gigue (ms) et la Perte de paquets. Chacun de ces paramètres revêt une importance capitale pour le responsable d'infrastructure parce qu'un seul paramètre peut affecter tout un groupe d'applications. Par exemple, prenons "la Perte de paquets" : quelle incidence aurait une perte de paquets trop importante pour la qualité des applications temps réel (VoIP, Streaming vidéo, ...) ? Sans nul doute, de graves problèmes de communication. Rappelons, à ce stade que la perte de paquets peut se produire pour des raisons liées à la congestion du réseau, mais aussi du fait de problèmes physiques (mauvais câblage, port de switch défectueux, …).
    - On pourrait aussi analyser les trois autres paramètres individuellement pour se rendre à l'évidence : la qualité de service réseau est un facteur stratégique à prendre en compte comme tel par le responsable d'infrastructure. Mais, si nous considérons uniquement le débit ou la bande passante, le problème est encore plus grave car, si ce paramètre n'est pas respecté, il est susceptible de perturber l'ensemble des applications. C'est ce paramètre qui risque de provoquer la congestion d'une liaison et, donc, la dégradation de performance des applications critiques ou métiers.

En fait, l'optimisation des quatre paramètres de QoS est cruciale pour garantir une expérience utilisateur satisfaisante et une utilisation efficace du réseau. En particulier, dans des environnements réseau où les applications critiques et métiers coexistent avec des applications gourmandes en bande passante.

Dans ce contexte, il est d'indispensable d'identifier l'ensemble des applications qui circulent sur le réseau d'entreprise, qu'elles soient en clair ou cryptées. Bien évidemment, les solutions que nous proposerons dans la dernière partie de ce livre blanc tiennent compte de cet aspect important des choses pour qu'aucune application ne soit classée comme inconnue.

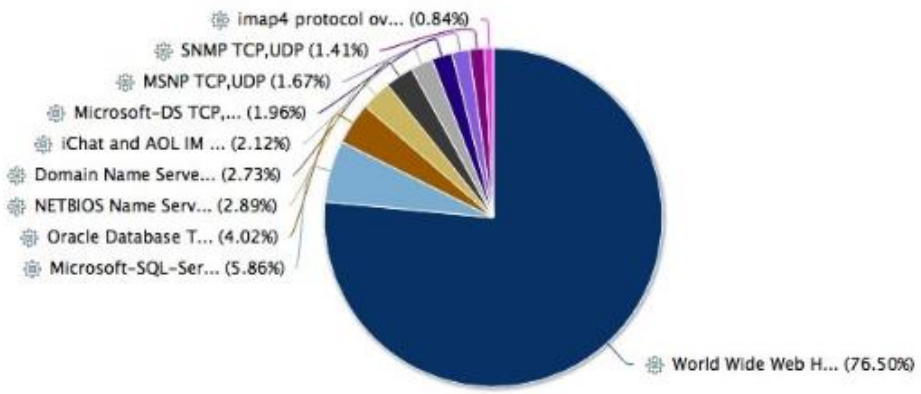
2) CAUSE SECURITE : ATTAQUES DE DENI DE SERVICE SUR LE RESEAU D'ENTREPRISE ET LES SERVEURS

Les attaques de déni de Service (DoS et DDoS) visent à saturer les ressources d'un réseau informatique, d'un serveur ou d'une application, rendant ces systèmes inaccessibles ou fonctionnant de manière inefficace pour les utilisateurs du réseau d'entreprise. Analysons la manière dont ces attaques agissent sur le réseau d'entreprise, les serveurs et les applications :

- **Surcharge de la Bande Passante** :
  - **DoS** : une attaque DoS peut inonder le réseau d'entreprise avec un volume massif de trafic, consommant toute la bande passante disponible et rendant difficile l'accès aux applications critiques et métiers.
  - **DDoS** : Les attaques DDoS utilisent un grand nombre d'ordinateurs, dénommés Zombies, répartis à travers Internet pour générer un trafic volumineux. La bande passante du réseau est submergée entraînant des retards et des interruptions dans l'accès aux applications critiques et métiers.
- **Saturation des Ressources Serveur** :
  - **DoS** : une attaque DoS peut concentrer un grand nombre de requêtes vers un serveur spécifique saturant ses ressources en CPU et Mémoire et provoquant un ralentissement ou un arrêt des services.
  - **DDoS** : en utilisant de nombreuses machines Zombies, une attaque DDoS peut surcharger les ressources d'un ou plusieurs serveurs internes affectant la disponibilté et la performance des applications métiers.
- **Epuisement des connexions Serveur** :
  - Certaines attaques DDoS, comme les attaques de SYN Flooding, peuvent épuiser les tables de connexions d'un serveur empêchant les nouvelles connexions légitimes d'être prises en compte et affectant la communication avec les applications critiques et métiers.

Dans le but de minimiser l'impact de ces attaques, les entreprises doivent prendre des mesures drastiques qui ne doivent pas reposer uniquement sur des firewalls et des systèmes de détection d'intrusion (sondes IPS). En effet, ces derniers peuvent aussi devenir des proies faciles pour les hackers qui peuvent en faire les cibles de leurs attaques malveillantes. Notre recommandation consiste à utiliser des services de protection DDoS spécifiques dimensionnés correctement comme nous le verrons plus tard dans le cadre des solutions que nous préconisons.

V) IDENTIFICATIONS DES GROUPES D'APPLICATIONS RISQUANT DE PERTURBER LES APPLICATIONS CRITIQUES ET METIERS



Plusieurs types d'applications peuvent concurrencer les applications critiques et métiers dans la course à la bande passante sur le réseau d'entreprise entraînant des problèmes de performance pour ces applications essentielles. Voici quelques catégories d'applications à surveiller :

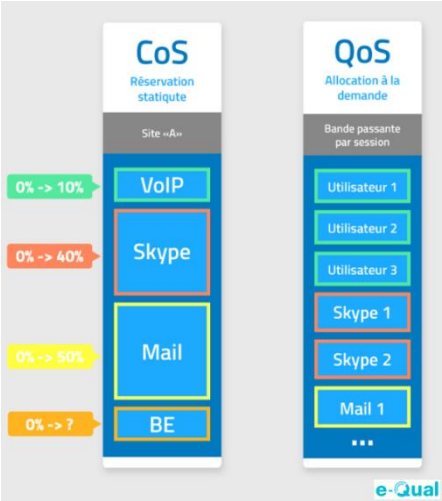
- **Applications en Streaming** :
  - Les services de streaming vidéo et audio consomment une grande quantité de bande passante. Par exemple, les flux de streaming de Youtube et Netflix.
- **Réseaux Sociaux et Messagerie Instantanée** :
  - Les applications de media sociaux, de messagerie instantanée et de visioconférence peuvent générer un trafic réseau considérable.
- **Téléchargement de fichiers volumineux** :
  - Les transferts de fichiers ou de données FTP, http download, et d'autres encore ont tendance du fait du principe TCP/IP à occuper la plus grande bande passante possible.
- **Mises à jour automatique** :
  - Les mises à jour automatiques des systèmes d'exploitation, des logiciels et des applications peuvent consommer sur un laps de temps plus ou moins long une grande partie de la bande passante.
- **Surf Internet non professionnel** :
  - Les téléchargements sur Internet personnels, la navigation Web à titre privé, le streaming personnel de vidéos, les jeux en ligne, le partage de fichiers P2P, …
- **Applications de sauvegarde et de synchronisation** :
  - Sauvegarde automatique des données vers un autre datacenter ou le cloud, synchronisation de fichiers, …

Grâce à un vrai contrôleur de QoS, il est possible d'éviter les baisses de performance liées à ces transferts de données de masse. Le responsable d'infrastructure peut mettre en œuvre des politiques de gestion du trafic basées sur la limitation, voire le blocage de certaines applications consommatrices de bande passante ou sur des créneaux horaires particuliers.

VI) ETUDE DES FAUSSES BONNES SOLUTIONS CENSEES PROTEGER LES APPLICATIONS CRITIQUES ET METIERS

Dans ce chapitre, nous allons étudier ce qui nous semble être trois fausses bonnes solutions qui pourraient induire en erreur les professionnels du réseau dans leur volonté de protéger leurs applications critiques et métiers sur le plan du contrôle de QoS. La plupart du temps, la bonne foi de ces professionnels n'est pas en cause, mais ils se sont juste fait duper par des spécialistes du marketing qui annoncent des fonctionnalités sur le papier alors que, dans la réalité, elles s'avèrent bien limitées. Nous en voulons pour preuve la fonction de contrôle de QoS qui est supposée exister dans un Routeur, un Firewall ou un équipement SD-WAN, alors que seul un service minimum est assuré. En effet, le routeur, le firewall et le sd-wan ont été conçus dans un but bien précis et ils ne peuvent pas supplanter un contrôleur de QoS dont la vocation première est d'assurer cette fonction ô combien importante pour la protection des applications critiques et métiers. Etudions, ci-après, le routeur, le firewall et le sd-wan par rapport à la fonction contrôle de QoS :

1) CONTRÔLE DU TRAFIC APPLICATIF PAR ROUTEUR

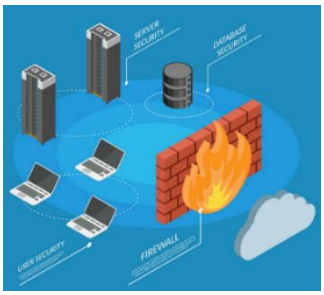


Les Classes de Services (CoS) des routeurs sont conçues pour prioriser et gérer le trafic réseau en fonction des quatre différents critères de qualité de services que nous avons vus au chapitre précédent. De notre point de vue, même si les Classes de Services peuvent avoir un intérêt, assez limité, pour certaines entreprises qui ne disposent pas de véritable contrôleur de QoS, dans un monde où les réseaux d'entreprise utilisent simultanément entre plusieurs dizaines et plusieurs centaines applications, les Classes de Services se trouvent vite dépassées et deviennent inopérantes. Voici quelques éléments qui en expliquent les raisons :

- **Manque de contrôle granulaire** :
    - Le principal reproche est lié au fait que les Classes de Services fonctionnent par groupe d'applications. On compte, selon les routeurs, entre 4 et 5 Classes de services. Les groupes d'applications correspondants sont les suivants : applications temps réel (VoIP, Vidéo temps réel, …), applications métiers, applications de sauvegarde et de transfert de données, applications de collaboration (messagerie instantanée, partage de fichiers, …) et navigation Internet. Cette liste n'est pas exhaustive, ce qui implique que de nombreuses applications appartiennent à une même classe de services, avec une gestion inhérente à cette classe de services, alors qu'elles n'ont rien à y faire. Le seul moyen de contrôler efficacement les applications du réseau consiste à les administrer individuellement grâce à un contrôleur de QoS digne de ce nom.
- **Trafic non conforme aux règles de CoS établies** :
    - Certains trafics réseau peuvent ne pas être correctement identifiés dans le champ de l'adresse IP adéquat. Dans ce cas, pour ces trafics inconnus, les priorités de traitement associées aux CoS ne sont pas appliquées.
- **Surcharge et Congestion du réseau** :
    - En cas de surcharge du réseau ou de congestion, les CoS ne peuvent garantir un traitement prioritaire en raison des ressources limitées du routeur dont la fonction principale de routage est privilégiée, ce qui peut conduire à des retards ou un traitement inégal du trafic réseau.
- **Evolution dynamique du trafic** :
    - Le trafic réseau peut évoluer rapidement et les CoS peuvent avoir du mal à s'adapter aux variations du trafic réseau.
- **Manque de ressources matérielles dans le routeur** :
    - Si les ressources matérielles du routeur (processeur, mémoire) sont insuffisantes pour gérer le volume de trafic ou les règles de QoS, cela peut entraîner des problèmes de gestion du trafic.
- **Pour chaque classe de services, le routeur fournit une réservation statique de bande passante** :
    - La CoS est un système basé sur un mécanisme de files d'attente
    - Chaque classe de service possède un niveau de priorité différent
    - La bande passante attribuée à chaque priorité est un pourcentage fixe du débit de la liaison réseau

Pour toutes les raisons évoquées, ci-dessus, on comprend aisément que la vocation d'un routeur consiste à assurer en priorité le bon fonctionnement du routage et la gestion de CoS n'est non seulement pas prioritaire, mais elle reste limitée eu égard au principe de files d'attente utilisé dans le contexte des applications modernes et à une gestion de CoS du trafic sortant uniquement. Par conséquent, il faut associer au routeur un vrai contrôleur de QoS afin d'administrer toutes les applications individuellement et, éventuellement, soulager les ressources du routeur en abandonnant purement et simplement la gestion de CoS au profit d'une gestion de QoS digne de ce nom.

2) CONTRÔLE DU TRAFIC APPLICATIF PAR FIREWALL



Un firewall ou un pare-feu est un élément de sécurité informatique essentiel dans un réseau d'entreprise. Son rôle principal est de contrôler le trafic entrant et sortant du réseau en veillant à ce que seuls les flux de données autorisés puissent passer et en bloquant les autres. Les firewalls classiques permettent le contrôle d'accès au réseau d'entreprise ou à Internet, le filtrage du trafic en fonction de règles bien définies, la prévention des intrusions et quelques fonctions limitées contre les attaques DDoS. Les firewalls nouvelle génération intègrent parmi d'autres fonctions, le filtrage d'URL, des fonctionnalités VPN sécurisées pour le télétravail, l'analyse comportementale du trafic pour prévenir les cybermenaces, la gestion centralisée des politiques de sécurité, des rapports détaillés et des fonctionnalités d'analyse pour évaluer la sécurité du réseau. En outre, certains firewalls offrent des capacités de gestion de Qualité de Service (QoS) limitées avec des fonctionnalités de contrôle et de priorisation du trafic rappelées, ci-après :

- **Attribution de priorités** :
  - A l'instar des routeurs, c'est à partir de critères de classification et de marquage sur adresse IP que le firewall attribue des priorités de traitement des paquets permettant une gestion différenciée du trafic
- **Allocation de bande passante** :
  - A l'instar des routeurs, le firewall gère la bande passante disponible en attribuant des quotas statiques de bande passante à chaque classe de services
- **Contrôle du trafic** :
  - A l'instar des routeurs, le trafic est effectué en fonction des politiques de "QoS" prédéfinies

Comme nous l'avons évoqué pour le routeur, le firewall n'est pas en mesure d'assurer une qualité de service telle qu'elle est réalisée par un contrôleur de QoS spécialisé. De notre point de vue, le firewall assure excellemment les fonctionnalités pour lesquelles il a été conçu, mais ne peut garantir un contrôle de QoS efficace dans un réseau d'entreprise moderne. Par ailleurs, à contrario d'un contrôleur de QoS, il ne peut garantir les fonctionnalités suivantes :

- Identification des applications en clair ou cryptées
- Gestion automatique de QoS individuelle par application, serveur ou poste de travail
- Gestion du trafic applicatif entrant et sortant à partir d'un seul point
- Attribution individuelle par application d'un minimum garanti de bande passante, d'un pourcentage de la bande passante disponible et d'un maximum (caping)
- L'optimisation de QoS doit se faire en combinant le Firewall avec un contrôleur de QoS

3) CONTRÔLE DU TRAFIC APPLICATIF PAR SD-WAN

Le SD-WAN (Software Defined Wide Area Network) est une nouvelle technologie apparue en 2005 aux USA qui transforme la manière dont les réseaux d'entreprise sont conçus, déployés et gérés. Depuis plus de 25 ans, c'était la technologie MPLS qui était le choix premier des opérateurs de réseaux en France et dans le monde pour interconnecter l'ensemble des sites d'une entreprise. Le SD-WAN, a modifié quelque peu l'hégémonie du MPLS, mais sans parvenir à le détrôner auprès des entreprises. Les principaux apports du SD-WAN viennent du fait que l'interconnexion des sites est réalisée au travers des liens Internet sécurisés par des tunnels IPSec et qu'il est possible de mixer divers types de connexions (ADSL, Fibre optique, câble, MPLS, 4G/5G, Satellite). D'autre part, c'est un moyen pour les utilisateurs des sites distants d'accéder directement à Internet et au cloud sans passer par un accès Internet centralisé. Les avantages du SD-WAN viennent donc à la fois de la possibilité d'interconnecter des sites par Internet et de mixer divers types de connexions. En revanche, les inconvénients sont multiples puisque Internet n'offre pas une qualité de service aussi performante que le MPLS et qu'il est nécessaire de déployer un boîtier SD-WAN sur chacun des sites du réseau d'entreprise, sans compter la sécurité à assurer sur chacun des sites, ce qui ajoute à sa complexité et au risque de pannes physiques pour les réseaux multi-sites de taille moyenne ou grande. C'est la raison pour laquelle dans les entreprises qui ont adopté le SD-WAN, le MPLS continue à prospérer et le mode hybride est privilégié. Avec le SD-WAN, nous avons vu apparaître des fonctionnalités liées au contrôle de QoS décrites, ci-après :

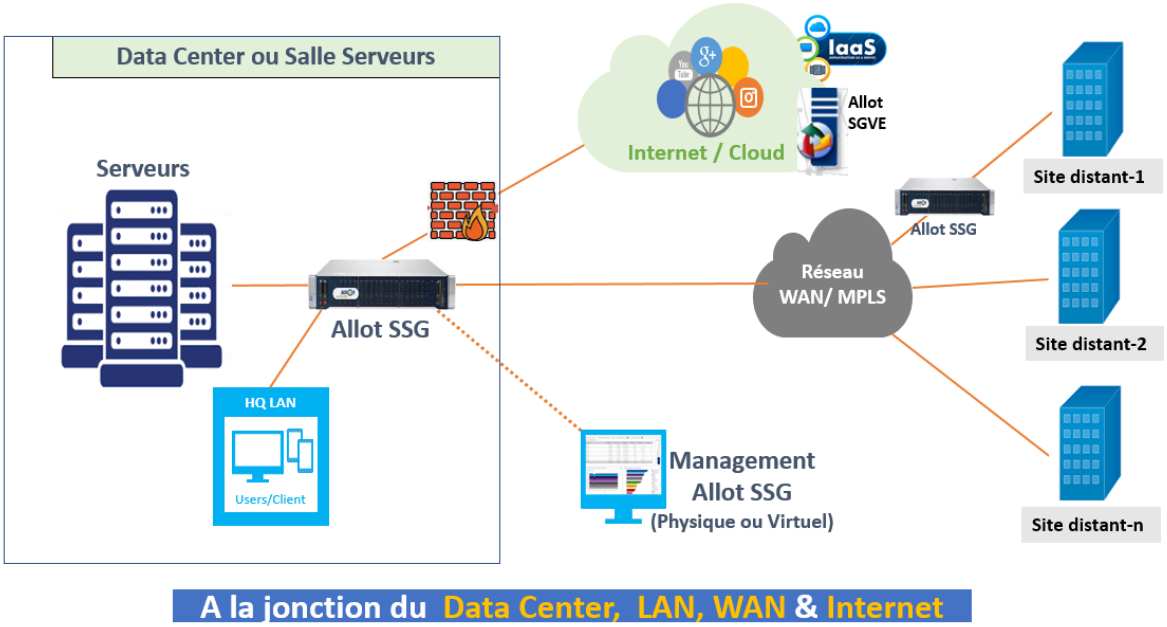
- **Priorisation du trafic** :
  - La priorisation du trafic à partir d'un boîtier SD-WAN est possible uniquement dans le sens sortant du trafic. Par conséquent, c'est le boîtier SD-WAN à l'autre extrémité qui doit assurer le contrôle de flux du trafic entrant. Par conséquent, pour les flux dirigés vers Internet et le cloud, il n'est possible d'assurer aucun contrôle des flux applicatifs entrants alors que ce sont eux qui représentent la grande majorité du trafic à contrôler.
- **Allocation de bande passante** :
  - L'allocation de bande passante, comme pour les priorités, est contrôlée uniquement dans le sens sortant des boîtiers SD-WAN, ce qui devient une difficulté lorsqu'il faut garantir spécifiquement un minimum de bande passante à une application critique ou métier.

Malheureusement, le contrôle de QoS du SD-WAN ne tient pas ses promesses si on le compare à un contrôleur de QoS spécialisé. En effet, pour contrôler les flux applicatifs de la meilleure manière, il faut vraiment disposer d'un moteur de QoS capable de gérer à la fois les applications par files d'attente et gérer la bande passante individuellement par application dans les deux sens du trafic à partir d'un seul point. De notre point de vue, l'optimisation de QoS ne peut se faire qu'en combinant SD-WAN et contrôleur de QoS.

VII) SOLUTIONS EFFICACES POUR PROTEGER LES APPLICATIONS CRITIQUES ET METIERS A PARTIR D'UN CONTRÔLEUR DE QOS

Dans les chapitres suivants, nous allons expliquer quelles sont les caractéristiques essentielles dont doit disposer un contrôleur de QoS dans le but d'assurer une véritable protection des applications critiques et métiers, de manière automatique, quel que soit l'état du trafic sur le réseau d'entreprise. Dans ce cadre, nous étudierons, dans un premier temps, les deux piliers de base que sont la visisbilité et le contrôle des flux applicatifs. Dans un deuxième temps, nous présenterons le volet sécurité intégré à la solution en décrivant la meilleure manière de détecter et corriger tous les types d'attaques de déni de services. Pour illuster notre propos, nous nous appuierons sur des produits de marque Allot qui est un des leaders mondiaux de l'intelligence et de la sécurité réseau. C'est à partir de ses produits performants, fiables et simples à déployer que nous construisons des solutions sur mesure pour nos clients.

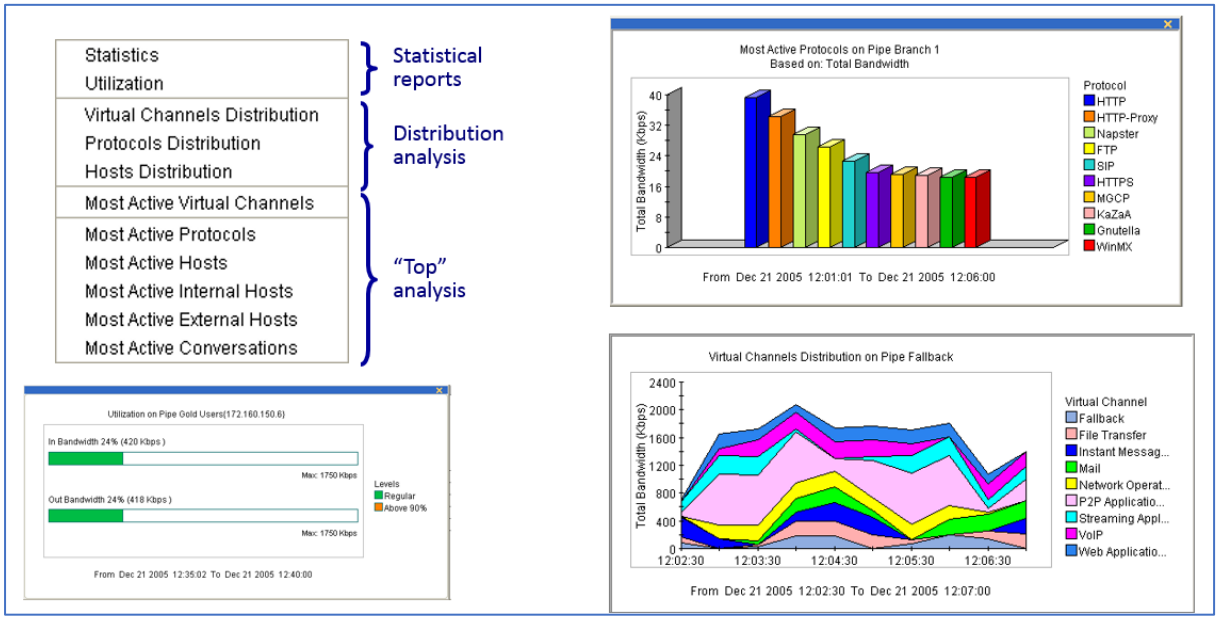
1) DEPLOIEMENT TYPIQUE D'UNE SOLUTION ALLOT DANS UN RESEAU D'ENTREPRISE MULTI-SITES



Dans le schéma, ci-dessus, une sonde Allot s'installe centralement dans un datacenter ou une salle serveurs. Cette sonde peut identifier et contrôler les flux applicatifs échangés entre, d'une part, les utilisateurs locaux et, d'autre part, les serveurs internes et Internet/Cloud. De la même manière, d'une part, les utilisateurs distants et, d'autre part, les serveurs internes et Internet/Cloud. Par ailleurs, si les serveurs de l'entreprise se trouvent sur le Cloud en

environnement Iaas, il est possible de placer une sonde virtuelle Allot SGVE sur le Cloud. Enfin, si on trouve des serveurs décentralisés sur un site distant, il est possible d'y installer une sonde Allot pour collecter le trafic transversal. Il faut noter que toutes les sondes Allot sont installées sur le LAN, même si elles controlent les flux WAN. Toutes les sondes déployées sur le réseau d'entreprise sont administrées par un logiciel de management dénommé Allot NetXplorer. En tout état de cause, insistons sur le fait que dans la majorité des déploiements Allot, une seule sonde placée dans le datacenter ou la salle serveurs suffit à collecter les flux applicatifs échangés au sein du réseau d'entreprise multi-sites.

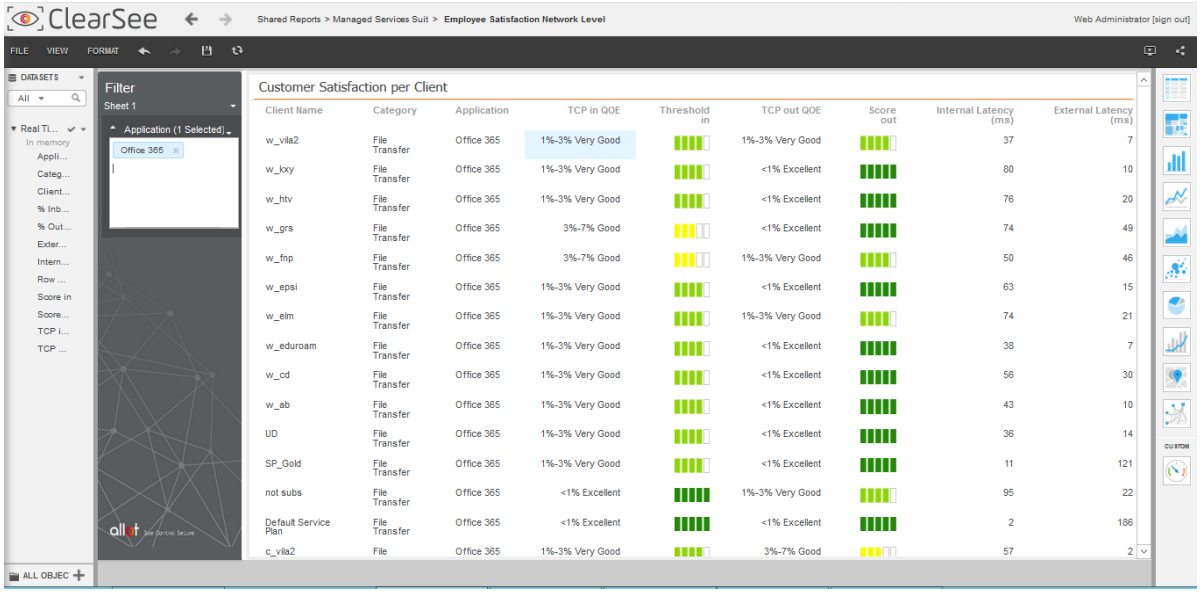
2) VISIBILITE TRADITIONNELLE SUR LES FLUX APPLICATIFS



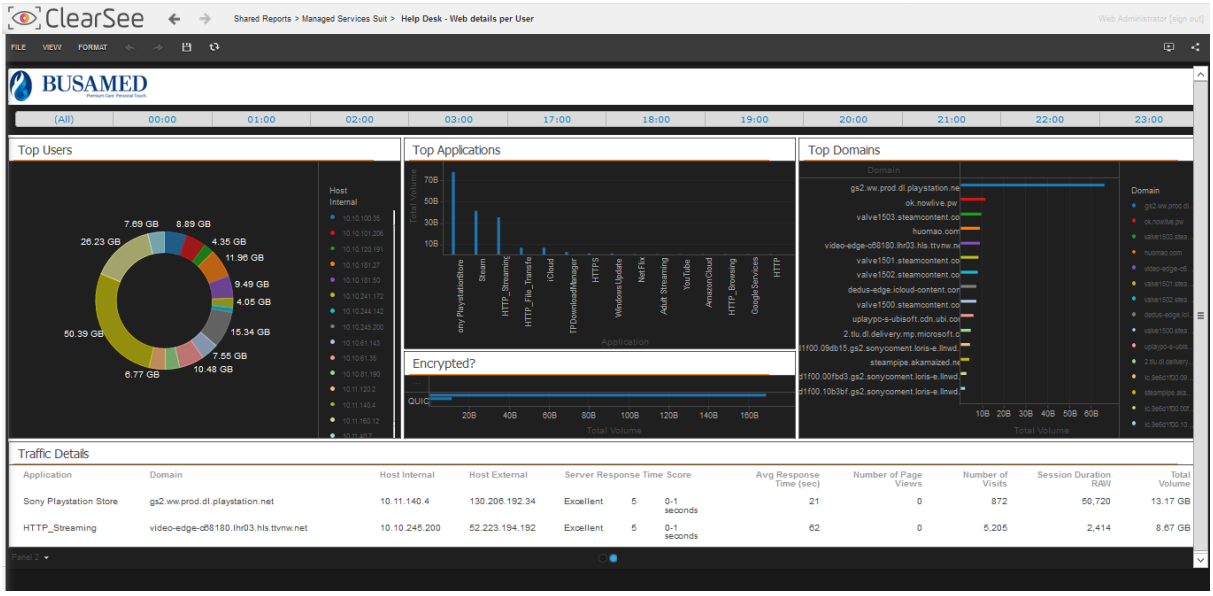
Dans le cadre de l'élaboration d'une politique de contrôle des flux applicatifs, la première étape consiste à réaliser un audit des flux. Cette opération va nous permettre d'identifier les applications qui consomment le plus de bande passante et les applications critiques et métiers. Tout ce travail est effectué en concertation avec certains utilisateurs du réseau qui sont particulièrement intéressés par le bon fonctionnement des applications critiques et métiers. Toutes les mesures statistiques effectuées sont en quasi temps réel puisque les échantillons collectés sont séparés de 30 secondes. Cette courte durée permet de réaliser, si nécessaire, des actions correctives sur le réseau et d'en analyser l'impact quasi instantanément. Par exemple, il est possible de suivre l'évolution d'une ou plusieurs applications en temps réel et d'analyser leur comportement.

De plus, dès que l'on voit l'évolution des applications au cours du temps, il est possible à tout moment de savoir en faisant un click droit sur elle, de savoir quelles sont les connexions associées à l'instant t ou cumulées et les différentes machines d'extrémité correspondantes (i.e. poste de travail et serveur). Ces fonctions temps réel constituent pour l'administrateur réseau des informations précieuses et des outils de dépannage vraiment efficaces.

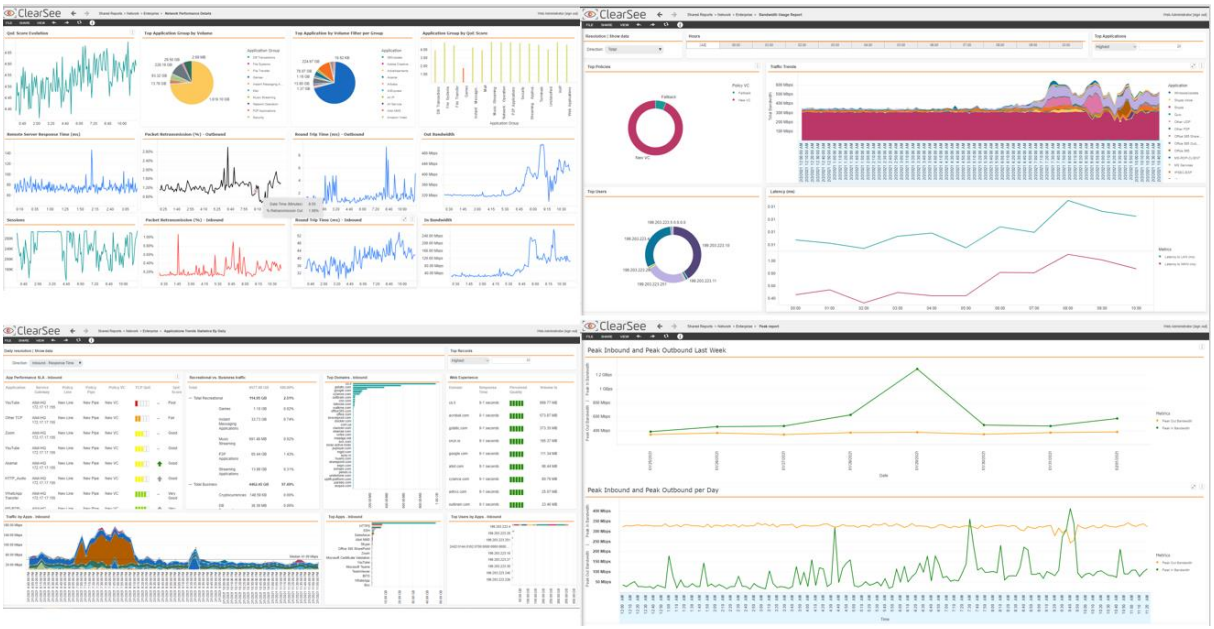
3) VISIBILITE ANALYTIQUE SUR LES FLUX APPLICATIFS



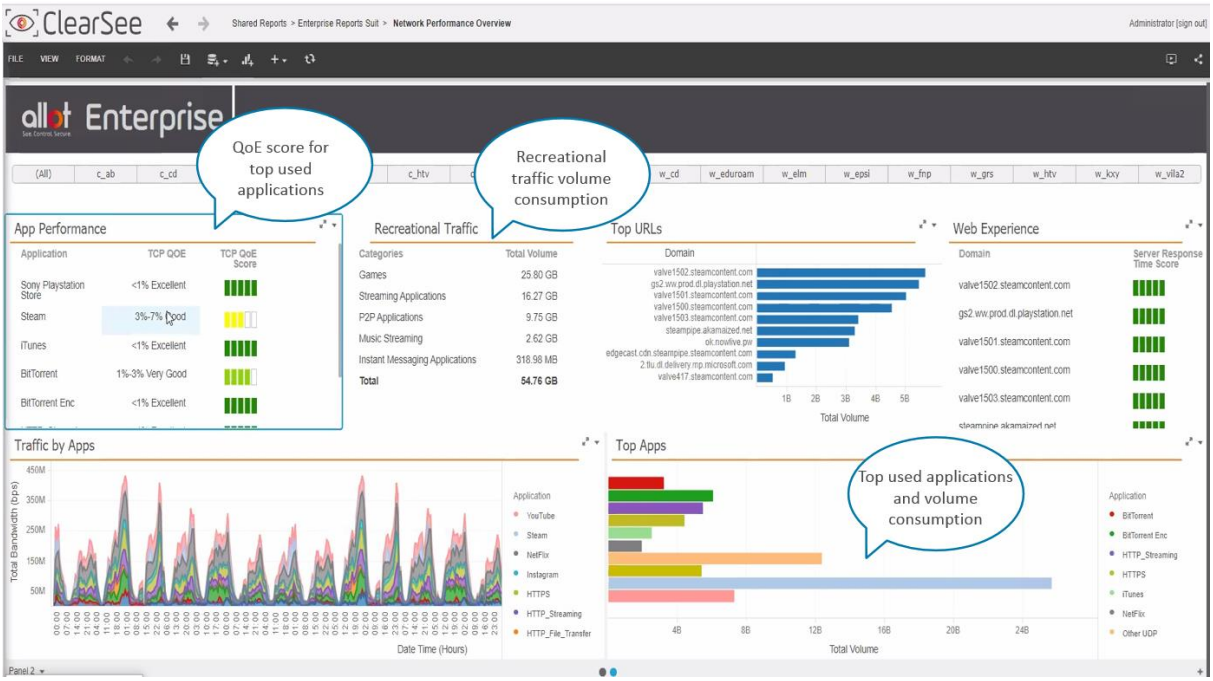
Dans le cadre de la visibilité analytique, grâce au module logiciel Allot ClearSee Analytics, nous pouvons constater que les graphes sont très complémentaires à la visibilité traditionnelle. Dans le graphe, ci-dessus, il est possible de connaître la satisfaction des utilisateurs par rapport à l'application Office 365. Les couleurs peuvent passer par le vert, le jaune, l'orange et le rouge pour détecter la présence d'une anomalie plus ou moins grave. Selon le graphe sélectionné, le module Allot ClearSee peut se comporter comme un système de supervision globale du trafic applicatif et, lorsqu'il détecte une anomalie, remonter à l'origine du problème grâce à sa forte granularité jusqu'à l'application, le poste de travail ou le serveur fautif.



La figure, ci-dessus, montre les détails des accès Internet pour l'ensemble des utilisateurs, les applications mises en œuvre et les URL correspondantes.



Dans la figure, ci-dessus, quatre graphes prédéfinis par le développement sur Allot ClearSee qui permettent au client de visualiser divers graphes utiles afin d'analyser instantanément le comportement des applications dans le réseau d'entreprise.



La figure, ci-dessus, est un graphe sur mesure réalisé par le client lui-même, c'est-à-dire que les vues qui y sont intégrées ont été assemblées selon ses desiderata.

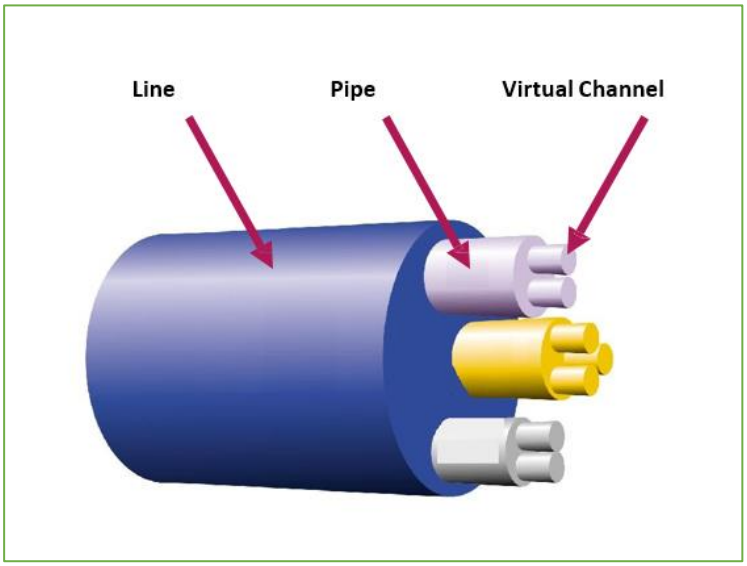
La combinaison des graphes traditionnels et analytiques permet d'assurer une maintenance préventive et curative du réseau d'entreprise en surveillant l'ensemble des applications circulant sur le réseau.

Par ailleurs, le module Allot ClearSee Analytics permet aussi d'identifier toutes les applications potentiellement malveillantes telles que Psiphon, Tor, OpenVPN, … qui sont susceptibles de traverser des firewalls et de suivre la détection et la "mitigation" des attaques DDoS.

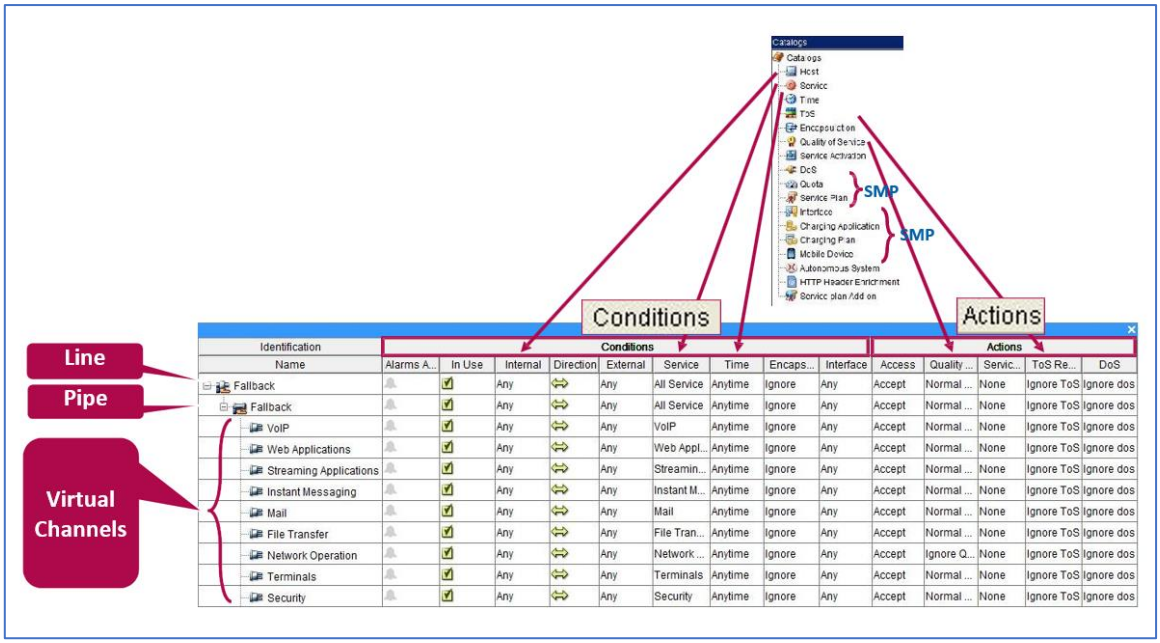
Notre expérience montre qu'une fois le module Allot ClearSee Analytics mis en place, nos clients trouvent des moyens nouveaux et innovants de créer de la valeur à partir des rapports d'analyse de réseau. Par exemple, un client multinational a utilisé la sonde Allot Service Gateway et ClearSee Analytics pour surveiller et contrôler de manière centralisée le trafic vers des milliers de points de vente depuis ses centres de données. En plus d'optimiser les transactions financières et les applications de collaboration commerciale, ils ont examiné le comportement en ligne des clients en magasin. Une opportunité a été découverte concernant les modèles d'achat : ils ont pris ces informations et les ont utilisées pour positionner des promotions ciblées de manière pertinente.

Notons aussi que le marketing Allot donne la possibilité d'Intégrer gratuitement le module Allot ClearSee Analytics complet destiné à 10 000 utilisateurs pour l'acquisition d'une solution de base incluant la visibilité traditionnelle et le contrôle de QoS.

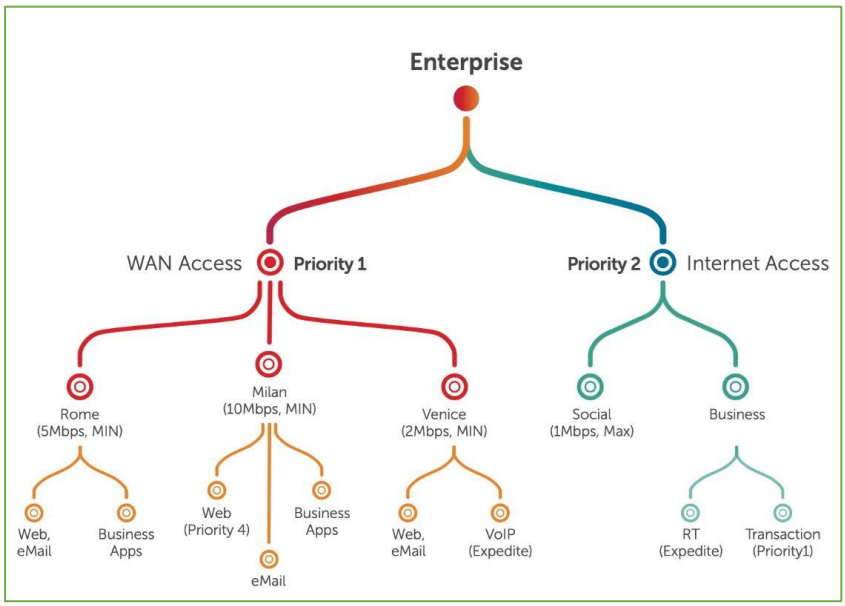
4) CONTRÔLE DE QOS SUR LES FLUX APPLICATIFS



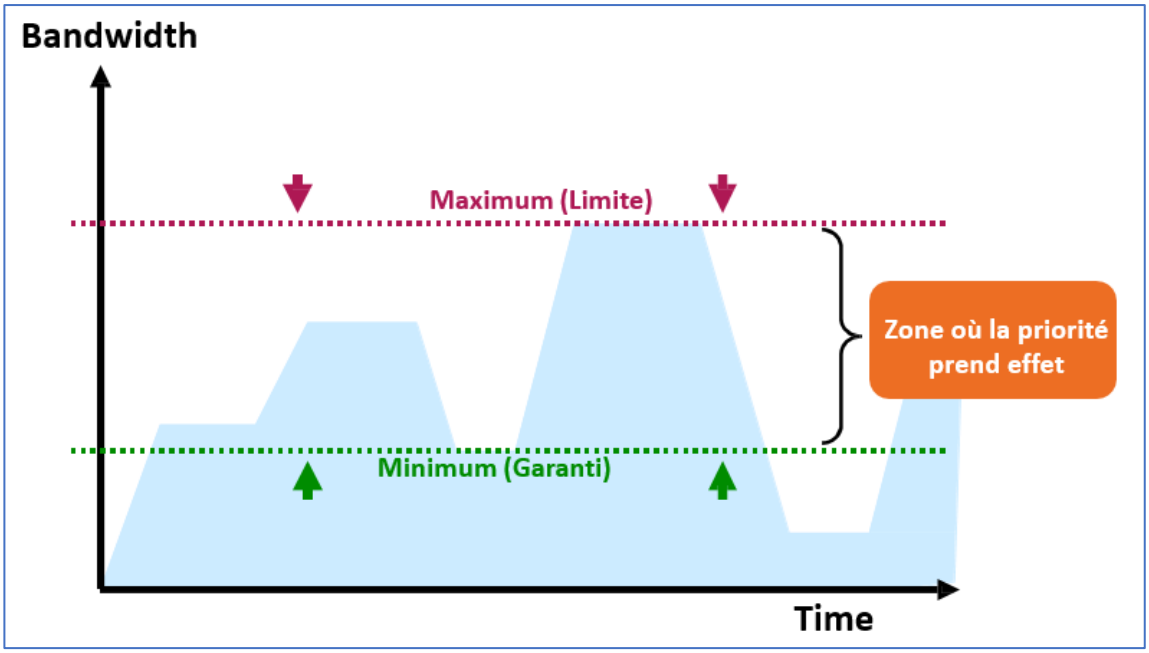
Dans le but de structurer le trafic pour faciliter son analyse et accélérer le processus de décision, Allot a hiérarchisé le trafic en fonction de trois objets dénommés Line, Pipe et Virtual Channel (VC). Pour fixer les idées par un exemple, Line pourrait représenter un opérateur, Pipe un site distant dépendant de cet opérateur et VC une application spécifique appartenant à ce site distant.



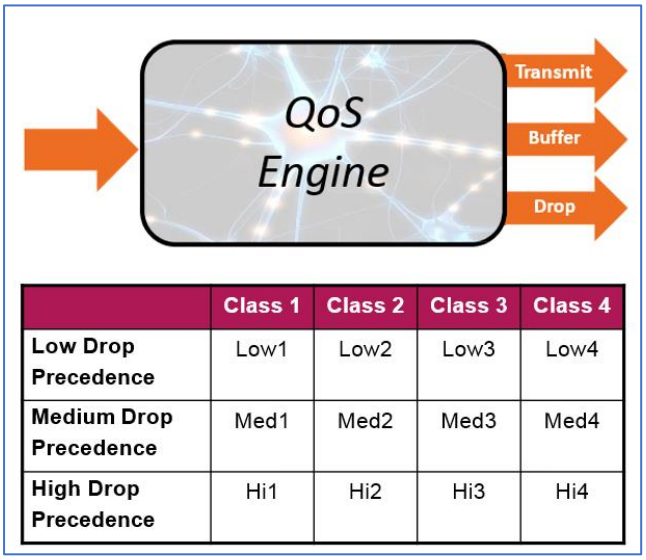
Dans la figure, ci-dessus, nous voyons de quelle manière les objets Line, Pipe et VC sont pris en compte par la solution Allot dans le cadre d'un ensemble de règles qui vont définir la politique de contrôle du trafic applicatif. Les colonnes de gauches constituent les **Conditions** qui permettent de filtrer le trafic, alors que les colonnes de droite constituent les **Actions** sur le trafic, et notamment, le contrôle de QoS tel que nous le détaillerons, ci-après.



La figure, ci-dessus, montre un exemple de structure typique permettant de contrôler à la fois un accès WAN et un accès Internet dans le but d'aligner les utilisateurs et les applications sur les priorités métiers de l'entreprise.



Le graphe, ci-dessus, explique de quelle manière une application critique peut bénéficier d'une bande passante garantie en cas de saturation du Pipe auquel elle appartient. Toute la bande passante au-dessus du minimum garanti peut être exploitée par les autres applications en fonction des 32 priorités disponibles.

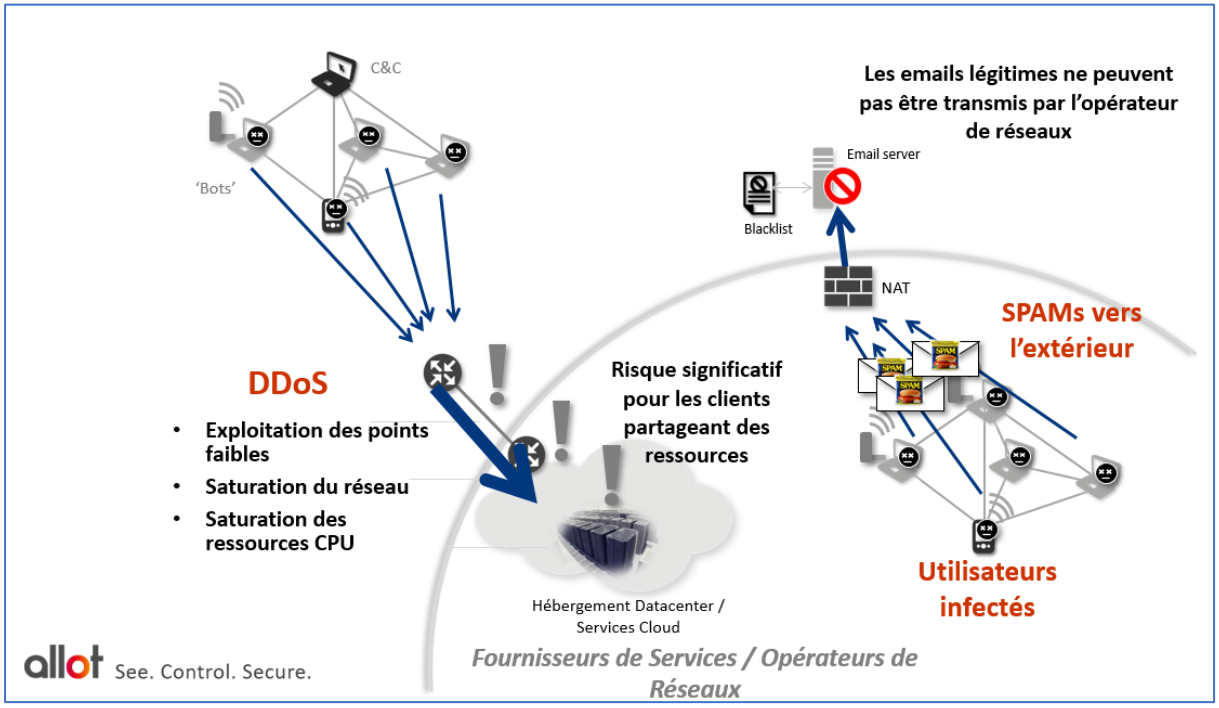


	Class 1	Class 2	Class 3	Class 4
Low Drop Precedence	Low1	Low2	Low3	Low4
Medium Drop Precedence	Med1	Med2	Med3	Med4
High Drop Precedence	Hi1	Hi2	Hi3	Hi4

En complément de la répartition de bande passante selon les maximums, les minimums garantis et les priorités, le moteur de QoS permet de contrôler le trafic en fonction de files d'attente dans le cas de surcharges de trafic. Ce contrôle de trafic est assuré en fonction du type d'application circulant sur le réseau simultanément. Les applications critiques et métiers bénéficieront du plus petit drop precedence, c'est-à-dire que les paquets IP correspondant à ces applications seront les derniers à être évincés du réseau.

5) PROTECTION ANTI-DDOS AVEC MITIGATION DES CYBERATTAQUES

Les entreprises, quelle que soit leur taille doivent protéger leur réseau d'entreprise en raison de l'ampleur et de la complexité croissantes des cyberattaques entrantes et sortantes qui sont conçues pour inonder les infrastructures réseau et perturber la disponibilité des services.



Dans la figure, ci-dessus, la solution anti-DDoS doit à la fois contrer les attaques venant de l'extérieur du réseau, et notamment, d'Internet, mais aussi les attaques internes liées aux machines infectées qui sont susceptibles de spammer vers l'extérieur.

La protection en temps réel Allot DDoS Secure permet de détecter et bloquer chirurgicalement les attaques par déni de service (DoS/DDoS) en quelques secondes, avant qu'elles ne puissent menacer ou perturber les services réseau.

La technologie NBAD (Advanced Network Behavior Anomaly Detection) identifie les attaques volumétriques en fonction des anomalies qu'elles provoquent par analyse comportementale du trafic réseau. La création dynamique de règles de mitigation et de filtrage chirurgical des paquets d'attaques permet d'éviter des blocages inutiles et au trafic légitime de circuler librement, en gardant le réseau d'entreprise accessible et protégé à tout moment.

La technologie HBAD (Advanced Host Behavior Anomaly Detection) identifie l'infection des hôtes et les comportements abusifs en fonction de l'activité de connexion sortante anormale et malveillante et des modèles de connexion, ce qui permet de maintenir le trafic anormal hors du réseau et de traiter la cause première de la menace ainsi que les symptômes. Dans ce cas, la solution anti-DDoS Allot détecte et bloque automatiquement la propagation des vers sortants, afin d'empêcher la mise sur liste noire du réseau et d'éliminer la charge de trafic supplémentaire sur le réseau.

Le module Allot ClearSee Analytics fournir une visibilité totale sur les menaces grâce à des alertes en temps réel qui signalent les menaces détectées et corrigées. Les dispositifs infectés peuvent également recevoir une notification. Allot fournit des journaux détaillés et personnalisables de mitigation des attaques, des analyses d'événements, des analyses d'infection d'hôte et des rapports de tendance/distribution pour prendre en charge la planification de la sécurité, la gestion des menaces et les décisions opérationnelles. Un tableau de bord unique du contrôleur de gestion surveille l'activité du réseau et des utilisateurs et gère la protection contre les menaces sur l'ensemble du réseau d'entreprise.

6) TEMOIGNAGES CLIENTS

VIII) CONCLUSION

Le présent livre blanc visait à démontrer le caractère indispensable d'un contrôleur de QoS, enrichi par des fonctionnalités de visibilité analytique et de protection anti-DDoS, dans un environnement d'entreprise multi-sites, pour garantir la protection et les performances optimales des applications critiques et métiers. En analysant les besoins spécifiques des entreprises modernes, des multiples défis rencontrés et des avantages d'un contrôle automatique de la QoS, ce document met en lumière la pertinence fondamentale du contrôleur de QoS par rapport aux trois fausses bonnes solutions qui ont été étudiées dans ce document : classes de services des routeurs, pseudo QoS des firewalls et pseudo QoS du SD-WAN.

Dans un monde où la quasi-totalité des entreprises de tailles moyennes ou grandes opèrent sur un réseau multi-sites, les performances et la sécurité des applications critiques et métiers sont primordiales. Ce livre blanc souligne la nécessité de hiérarchiser, prioriser, optimiser et garantir dans certains cas le trafic réseau applicatif, dans le but d'assurer une protection adéquate aux applications critiques et métiers.

En conclusion de ce livre blanc, il est indéniable que le contrôleur de QoS et ses fonctionnalités annexes détaillées dans ce document, se révèle être un pilier central pour garantir la protection des applications critiques et métiers dans un réseau d'entreprise multi-sites.

Bien entendu, avant que les entreprises qui ont été convaincues par notre livre blanc investissent dans un contrôleur de QoS, nous leur demandons instamment de faire les bons choix suivants :

- Tout d'abord, il s'agit de sélectionner des produits qui sont à la fois performants, faciles à déployer autant qu'à utiliser et fiables dans la durée. C'est le cas des produits de la société Allot qui s'impose depuis 26 ans comme un leader dans le monde de l'intelligence et de la sécurité réseau. Allot vend ses produits dans plus de 50 pays et à bâti sa notoriété à la fois auprès des entreprises et des opérateurs.
- En second lieu, il faut sélectionner un intégrateur de services WAN, Datacenter et Cloud capable d'intégrer les produits Allot. C'est le cas de la société MERISAC, partenaire historique de la société Allot depuis 20 ans, et qui possède toutes les certifications utiles pour vendre, installer, former et assurer un support de qualité auprès de ses clients.

Pour contacter MERISAC :

- Secrétariat : 01 49 33 73 75
- Urgence : 06 60 12 64 51
- Mail : merisac@merisac.com
- Page contact : https://www.merisac.com/contact-us/
- Site Web https://www.merisac.com :