



# Les pare-feu ne sont pas qu'une affaire de sécurité

Les applications Cloud forcent les pare-feu à favoriser  
la productivité



## Présentation

L'avènement du Cloud Computing décuple les conflits d'accès à la bande passante dans la mesure où les applications internes vont elles aussi migrer sur le cloud. Les entreprises ne peuvent pas déployer de nouvelles solutions à chaque nouveau défi lancé par le cloud. La solution réside dans la différence entre ce que les pare-feu « font » et ce que les pare-feu « peuvent faire ».

Si nous arrêtons de penser que les pare-feu ou les UTM ne servent qu'à bloquer le mauvais trafic, nous pourrions peut-être les transformer en solutions de productivité fonctionnant comme des outils d'exploitation. En les faisant fonctionner au niveau des couches 7 (application) et 8 (utilisateur), les pare-feu peuvent visualiser le trafic des applications non pas avec une association désuète port-protocole, mais avec une fonction dynamique qu'ils peuvent activer efficacement.

Grâce aux 4 éléments suivants : qui (utilisateur), quoi (application), quand (heure) et combien (bande passante), les pare-feu peuvent avoir une visibilité et un contrôle des couches 7 et 8 en se basant sur l'heure et les besoins en bande passante afin de réduire les pics et les creux de la demande en bande passante, donner priorité aux applications blanches, bloquer les applications noires ou contrôler intelligemment l'accès aux applications grises. Ainsi, ils augmentent la productivité, et créent un environnement de travail attrayant.

# Contents

Introduction.....	1
Le défi des applications dans l'ère du Cloud .....	2
Les pare-feu ne sont pas qu'une affaire de sécurité .....	4
Gestion des 4 éléments : Application, Utilisateur, Heure, Bande passante .....	5
Analyse des 4 éléments .....	6
Cyberoam vous prépare au Cloud .....	7





Alors que la principale préoccupation de l'industrie se concentre sur les éventuels défis de sécurité introduits par le Cloud, les défis de productivité ne vont pas tarder à assaillir les entreprises. À l'exception de la bande passante allouée aux applications vitales telles que la téléphonie sur IP et la vidéoconférence, les entreprises ne sont pas équipées pour assurer un accès aux applications à tous les utilisateurs.

## Introduction

Avec l'avènement du cloud, la tradition est mise à rude épreuve.

Les applications traditionnellement localisées « au sein » du réseau sont désormais « à l'extérieur » sur le cloud, se disputant pour la première fois la bande passante avec des applications externes. Les pare-feu ont toujours été envisagés comme des solutions dédiées à la sécurité. Aussi, les entreprises ont aujourd'hui du mal à répondre aux conflits d'accès à la bande passante causés par la migration des applications sur le cloud.

Gérer l'accès aux applications n'est pas une mince affaire étant donné la multitude d'applications, leur disponibilité sur le Web et l'adoption du SaaS (Software as a Service : logiciel en tant que service) pour les applications grand public.

À cela s'ajoute la complexité d'accès et de contrôle des applications. En brouillant la distinction jusqu'alors claire entre les applications internes hébergées dans les centres de données des entreprises et les applications externes disponibles sur la toile, le défi que pose la gestion de l'accès aux applications ainsi que leur contrôle devient beaucoup plus complexe, et fait l'objet d'une attention particulière.

Alors que la principale préoccupation de l'industrie se concentre sur les éventuels défis de sécurité introduits par le Cloud, les défis de productivité ne vont pas tarder à assaillir les entreprises. À l'exception de la bande passante allouée aux applications vitales telles que la téléphonie sur IP et la vidéoconférence, les entreprises ne sont pas équipées pour assurer un accès aux applications à tous les utilisateurs.

Pourtant, les entreprises ne peuvent pas se permettre d'augmenter aveuglément le nombre de solutions pour répondre aux défis du Cloud. La solution permettant de garantir Application et QoS (Qualité de Service) repose dans les pare-feu et UTM (Unified Threat Management, Traitement unifié de la menace)<sup>1</sup>. Les entreprises ont besoin de sortir de leur pensée traditionnelle et cloisonnée, à savoir des réseaux limités en matière d'applications, aujourd'hui en voie de disparition. Les pare-feu doivent évoluer pour répondre aux nouvelles exigences en allant au-delà des simples règles « autorisation/blocage d'applications » afin de fournir des contrôles granulaires qui appliquent une QoS pour chaque application et chaque utilisateur, chose qui n'avait jamais été envisagée auparavant.

L'approche actuelle de la plupart des pare-feu, qui consiste à ignorer les couches 7 (application) et 8 (utilisateur) ou à dissocier ces 2 couches avec quelques pare-feu gérant la couche 7 et solutions IAM (Identity and Access Management, Gestion des Identités et des Accès) gérant la couche 8, devrait faire céder les entreprises face aux pressions liées à la bande passante et à la productivité en découlant.

La nouvelle approche du pare-feu, qui consisterait à englober de manière très complète les 4 éléments (application, utilisateur, heure et bande passante) pouvant être simplement gérés par la visibilité et les contrôles des couches 7 et 8, fournit la productivité nécessaire en poussant les pare-feu au-delà de leur démarche traditionnelle axée sur la sécurité.

<sup>1</sup> Dans le présent livre blanc, le terme « pare-feu » fera référence à la fois aux pare-feu et aux solutions UTM, dans la mesure où les pare-feu font partie intégrante des solutions UTM.



Même si les applications nous facilitent la vie au travail et nous divertissent à la maison, elles représentent une véritable menace en matière de sécurité et de productivité.

## Le défi des applications dans l'ère du Cloud

L'utilisation des applications au fil du temps représente l'histoire de la communication, de l'évolution des connaissances, du divertissement et de la collaboration sur la toile mondiale.

### Évolution de la communication et des connaissances

Internet était à l'origine un moyen de communication instantanée via email. Aujourd'hui, avec une quantité incalculable de sites qui emmagasinent chaque jour de plus en plus de données, Internet s'est transformé en véritable base de connaissances. Jusqu'ici, cela n'a posé aucun problème, même si la plupart des employés des entreprises ont accès à Internet. Pour faciliter les choses, les applications ont suivi un schéma prévisible de l'utilisation port-protocole.

### Divertissement

Avec des millions de gens en ligne, le divertissement a rapidement suivi le mouvement en proposant des applications de jeux, de tchat, et de téléchargement audio et vidéo. Les pertes de productivité se sont fait sentir de deux manières. Lorsque certains employés se permettaient d'utiliser des applications non professionnelles de jeux, de téléchargement audio et vidéo via les réseaux Peer-to-Peer (Kazaa, etc.), les applications vitales de l'entreprise quant à elles souffraient d'un manque de bande passante.

Les entreprises se sont donc rendu compte que l'accès aux applications devait être contrôlé, non seulement en raison des nombreuses menaces que l'utilisation de telles applications présentait pour le réseau, mais également en raison des téraoctets de bande passante qu'elles consommaient et l'importante perte de productivité que cela impliquait. Le brouillage de port a donc véritablement commencé, et est venu s'ajouter à la complexité du contrôle des applications.

### Collaboration

La collaboration a suivi de près l'apparition discrète des outils de partage de fichiers pour répondre aux problèmes de transfert de fichiers volumineux par email. Alors que Microsoft Sharepoint et Google Docs se présentaient comme des exemples d'outils de travail collaboratifs purs, les solutions WebEx, Adobe Connect et GoToMeeting rassemblaient déjà les gens, proposaient des emplacements dédiés à la vente et au marketing pour la communication et le travail collaboratif en interne.

La collaboration est de plus en plus adoptée chaque année. En effet, elle facilite le transfert, accélère le rythme de travail, permet d'échanger avec le monde entier et de réduire les coûts de transport.

Aujourd'hui, c'est tout un mélange d'applications (personnelles, professionnelles, audio, vidéo, collaboratives, de divertissement, de communication instantanée) qui prennent d'assaut le Web, et donc les entreprises. Les applications SaaS, telles que Salesforce, ERP de NetSuite, Birt (avec Business Intelligence), et les autres, de plus en plus utilisées, telles que Facebook, Twitter, You Tube et les messageries instantanées, qui nous facilitent la vie au travail et nous divertissent à la maison, représentent une véritable menace en matière de sécurité et de productivité.



Pour relever le défi, les pare-feu doivent changer leur manière de gérer les besoins des entreprises : c'est-à-dire passer de l'objectif traditionnel qui consiste à « bloquer les mauvaises choses » à un nouvel objectif qui consiste à « autoriser les bonnes choses ».

### Cloud Computing

Le Cloud Computing annonce une nouvelle ère. Une ère dans laquelle d'importants changements ont lieu dans notre manière de regrouper, d'échanger, de stocker et de récupérer les données. Ce qui à l'origine était confiné dans le réseau est désormais en train de migrer en dehors de ce dernier.

Le SaaS a peu à peu réussi à se faire adopter par le grand public. Avec le Cloud, la mobilité des applications à l'extérieur du réseau est accélérée, dans la mesure où la plupart des applications internes peuvent être localisées en dehors de ce dernier. Ce phénomène a une incidence importante sur la consommation de bande passante dans les entreprises.

La préparation à l'adoption, la transition en douceur et la réussite du cloud computing dépendent en grande partie de la disponibilité et de la facilité de l'accès aux applications et données hébergées qui vont désormais commencer à concurrencer les applications externes existantes.

Les entreprises vont avoir du mal à trouver un équilibre entre les trois catégories d'applications : professionnelles (applications blanches) ; non-professionnelles (applications noires) ; et socioprofessionnelles (applications grises).

En l'absence de directives claires, les applications vitales (blanches) finiront par se disputer la bande passante avec les applications non vitales (noires ou grises). Le travail en pâtit, et la productivité que le cloud était censé améliorer s'affaiblit. Plus la bande passante est sollicitée, plus les coûts augmentent.

Pour relever le défi, les pare-feu doivent changer leur manière de gérer les besoins des entreprises : c'est-à-dire passer de l'objectif traditionnel qui consiste à « bloquer les mauvaises choses » à un nouvel objectif qui consiste à « autoriser les bonnes choses ».

## Les pare-feu ne sont pas qu'une affaire de sécurité

Les pare-feu traditionnels contrôlaient l'adresse source et destination, les ports et les protocoles. Savoir quel paquet entraît ou sortait du réseau ne semblait pas très important, tant que ce dernier respectait les règles créées pour ces paramètres, puisque les applications elles-mêmes utilisaient l'association port-protocole.

En outre, il ne semblait pas non plus important de savoir qui recevait le trafic dans l'entreprise tant que l'adresse source ou destination était acceptable parce que, finalement, peu de gens avaient accès à Internet.

Les choses ont changé lorsque les applications ont augmenté de façon exponentielle en nombre et en variété, et qu'il a fallu contrôler les applications pénétrant dans les entreprises. Les choses ont davantage changé lorsque l'accès à Internet s'est répandu dans toute l'entreprise : tout le monde n'avait pas besoin d'accéder aux applications. Ainsi, l'utilisateur est devenu un élément important pour les pare-feu.

Le fait que les pare-feu ne pouvaient plus attendre des applications qu'elles utilisent une association standard port-protocole était particulièrement important. Avant, toutes les applications HTTP utilisaient le port 80, et toutes les applications SSL utilisaient le port 443.

Avec la multiplication des applications, certains ont choisi de ne pas passer par les ports traditionnels pour une plus grande efficacité du transfert des paquets, tandis que d'autres ont choisi cette voie pour contourner les limitations du pare-feu. C'est à ce moment-là que le port hopping (saut de ports) a fait son entrée.

Sans oublier les sites et les logiciels de contournement de proxy comme ByPassU, YouMask et UltraSurf qui contournent les pare-feu traditionnels, et permettent aux utilisateurs de surfer sans restriction sur le Web.

Mais avec des applications vitales hébergées sur le réseau, de simples règles permettant de bloquer les applications noires et même grises faisaient l'affaire avec plus ou moins d'efficacité, et les aspects de sécurité liés à l'augmentation des applications demeuraient le centre d'intérêt. La nécessité de gérer la bande passante en fonction des applications ne se faisait pas sentir.

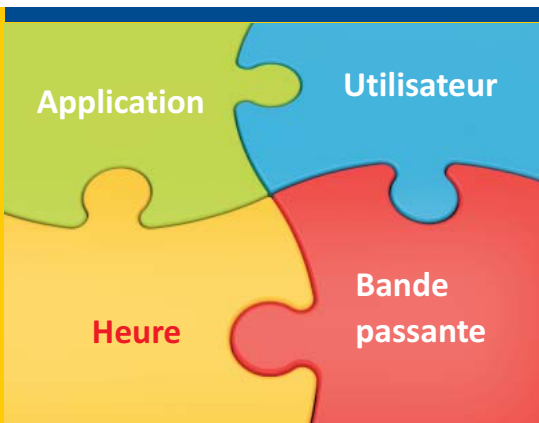
Avec le SaaS, la collaboration et le Cloud faisant migrer les applications internes en dehors du réseau, la lutte acharnée pour la bande passante est déjà perceptible. Ces applications seraient donc là-haut, dans le cloud, en train de se battre avec les applications externes pour obtenir un peu de bande passante.

Si l'on imagine que toutes les données sont migrées dans le cloud, la bande passante ne sera vraisemblablement pas suffisante. Le fait que certaines applications (audio, vidéo, conférence et certaines fonctions de collaboration) consomment beaucoup de bande passante est particulièrement important. En effet, les entreprises vont continuellement manquer de bande passante si leur pare-feu n'a pas été en mesure d'identifier les applications et les utilisateurs.

Il ne s'agit donc plus seulement d'assurer la disponibilité des applications, mais également d'optimiser la bande passante si l'on veut continuer à contrôler les coûts. Ainsi, la gestion des 4 éléments : qui (utilisateur), quoi (application), quand (heure) et combien (bande passante), qui permet une visibilité et un contrôle des couches 7 et 8 en se basant sur l'heure et les besoins en bande passante, devient nécessaire pour à la fois améliorer la productivité et contrôler les coûts.



Avec la multiplication des applications, certains ont choisi de ne pas passer par les ports traditionnels pour une plus grande efficacité du transfert des paquets, tandis que d'autres ont choisi cette voie pour contourner les limitations du pare-feu. C'est à ce moment-là que le port hopping (saut de ports) a fait son entrée.



L'intégration de pare-feu avec les 4 éléments : application-utilisateur-heure-bande passante garantit la création de l'ensemble de règles de pare-feu le plus simple et le plus efficace répondant aux besoins en QoS de l'accès aux applications.

## Gestion des 4 éléments : Application - Utilisateur - Heure - Bande passante

L'intégration de pare-feu avec les 4 éléments : application-utilisateur-heure-bande passante garantit la création de l'ensemble de règles de pare-feu le plus simple et le plus efficace répondant aux besoins en QoS de l'accès aux applications. En réservant la bande passante aux applications vitales et en contrôlant l'utilisation des applications moins importantes, les pare-feu peuvent désormais réduire les pics et les creux de la demande en bande passante et garantir la disponibilité de l'application et la QoS, et ainsi améliorer l'expérience de l'utilisateur.

Même si les 4 éléments sont essentiels, la bande passante est l'élément commun qui constitue la base permettant de gérer efficacement les 3 autres.

### Application

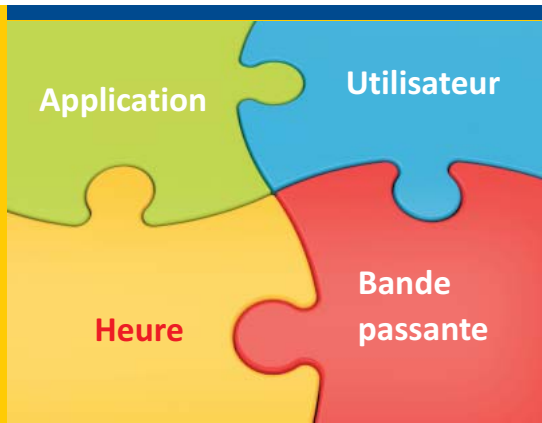
Les pare-feu vont devoir faire la distinction entre les différentes applications. Voici une répartition des applications en 3 catégories (noires, blanches et grises).

- Professionnelles (blanches) - Les applications entièrement professionnelles (telles que les applications de téléphonie sur IP, de Salesforce) devraient être numéro dans la hiérarchie organisationnelle de la bande passante. Elles devraient donc être prioritaires dans l'attribution de bande passante, quelle que soit l'heure de la journée.
- Non professionnelles (noires) - Les applications de divertissement exclusivement (telles que iTunes et les applications P2P) se verront probablement attribuer la priorité la plus faible en termes de bande passante. Les entreprises peuvent également les bloquer entièrement, notamment en cas de P2P. Ou, en raison de la demande croissante pour certaines applications de médias sociaux et la nécessité de construire un environnement de travail attrayant, elles peuvent également limiter le temps de disponibilité et restreindre l'accès à certains groupes d'utilisateurs.
- Socioprofessionnelles (grises) - La vraie question se pose avec ces applications grises. En effet, elles n'étaient à l'origine destinées qu'à un usage personnel (messageries instantanées, outils de médias sociaux comme Facebook et You Tube), mais elles ont évolué et représentent aujourd'hui un mélange entre le professionnel et le divertissement. Les utilisateurs d'aujourd'hui sont susceptibles d'utiliser certaines applications pour effectuer des tâches à la fois professionnelles et personnelles. Facebook, par exemple, était à l'origine une application de médias sociaux. L'application se retrouve aujourd'hui avec un nombre croissant d'utilisateurs pour son tchat et sa messagerie électronique. La création de communautés de partenaires ou de clients sur Facebook fait désormais partie intégrante du processus marketing et communication.

### Utilisateur

Alors que Salesforce, Microsoft Sharepoint ou Google Docs devraient toujours bénéficier d'un accès prioritaire, et que l'accès à iTunes devrait toujours être limité ou interdit, les choses ne sont pas aussi claires lorsqu'il s'agit d'applications de médias sociaux (You Tube, LinkedIn) et de transferts de fichiers (messageries instantanées). C'est là que la reconnaissance de l'utilisateur prend tout son sens.

Prenons le cas où You Tube est utilisé par le service responsable du marketing et des ventes de l'entreprise. On pourrait penser qu'une simple règle autorisant ce service à accéder à You Tube et l'interdisant à tous les autres ferait l'affaire. Mais que se passe-t-il si, à cause de ça, la téléphonie par IP, les conférences WebEx ou la collaboration Sharepoint n'ont plus assez de bande passante ?



Avant de mettre en place un système de contrôles avec une matrice complexe impliquant l'application, l'utilisateur, l'heure et la bande passante, il convient d'abord d'observer le trafic et de s'intéresser de plus près au schéma d'utilisation

Outre la couche 7 (application), les entreprises auraient maintenant besoin d'inclure la couche 8 (utilisateur) dans les règles de pare-feu. Ainsi, l'entreprise peut déterminer la bande passante minimale nécessaire pour l'application et appliquer la règle de pare-feu en conséquence, en attribuant la bande passante en priorité aux applications vitales.

### Heure

L'heure est le troisième élément important pour les règles de pare-feu. Pour les applications critiques en termes de bande passante et non en termes de temps, une restriction de leur accès à certaines heures de la journée allégera la consommation de bande passante.

Pour l'accès à You Tube, par exemple, l'entreprise aurait intérêt à fixer une règle avec une disponibilité de bande passante maximale au-delà de laquelle l'application ne peut plus utiliser la bande passante de l'entreprise. En outre, l'entreprise peut prédéfinir des heures en dehors des heures de travail au cours desquelles elle accorde plus de bande passante à l'application grise. Cela permet d'éviter de saturer la bande passante.

Par conséquent, intégrer les 4 éléments dans le pare-feu constitue le meilleur moyen pour gérer les applications dans le cloud.

## Analyse des 4 éléments

Avant de mettre en place un système de contrôles avec une matrice complexe impliquant l'application, l'utilisateur, l'heure et la bande passante, il faut analyser le trafic.

Dans un premier temps, tout ce que l'entreprise possède, c'est un graphique indiquant le schéma de consommation de la bande passante (pics et creux) au sein de l'entreprise. Mettre en place une règle qui favorise la productivité de l'entreprise sans pour autant la limiter nécessite qu'on s'intéresse de plus près au schéma d'utilisation se concentrant sur les facteurs suivants :

1. Distinguer parmi les applications
  - a. Les applications professionnelles (ou applications blanches)
  - b. Les applications non professionnelles (ou applications noires)
  - c. Les applications à la fois professionnelles et personnelles (ou applications grises)
2. Distinguer parmi les utilisateurs
  - a. Les utilisateurs-clés, en fonction de leur position ou rôle dans l'entreprise
  - b. Les utilisateurs consommant beaucoup de bande passante (avec une distinction entre les utilisations professionnelles et non professionnelles)
  - c. Les utilisateurs et services ayant des besoins spécifiques (ex. : application de médias sociaux pour le service responsable du marketing et des ventes)
3. Étudier le caractère critique de l'heure : relever les heures auxquelles les applications professionnelles vitales et les applications non professionnelles sont utilisées
4. Identifier les besoins en bande passante : lister la bande passante nécessaire pour chaque application professionnelle importante

En répondant à ces questions, l'entreprise peut savoir qui (élément utilisateur) utilise quelle application (élément application), à quel moment (élément heure) et quelle quantité de bande passante totale et individuelle (élément de bande passante) est nécessaire.

Avec les données de ces 4 éléments, les services informatique peuvent convoquer les chefs des différents services afin de négocier les contrôles et les restrictions pour équilibrer les pics et les creux.



Cyberoam est le seul UTM qui fonctionne sur les couches 2 à 8, offrant visibilité et contrôle des couches 7 (application) et 8 (utilisateur), quelle que soit l'origine de l'application.

## Cyberoam vous prépare au Cloud

Cyberoam est une solution de gestion unifiée des menaces (UTM, Unified Threat Management) qui a toujours su maintenir l'équilibre entre la sécurité et la productivité au sein de l'entreprise.

Il est le seul UTM qui fonctionne sur les couches 2 à 8, offrant visibilité et contrôle des couches 7 (application) et 8 (utilisateur), quelle que soit l'origine de l'application. Parallèlement, il offre une sécurité unifiée, en permettant aux entreprises de créer des règles pour toutes les fonctionnalités UTM, y compris la gestion de la bande passante à partir de la page dédiée au pare-feu.

Ainsi, il est en mesure de gérer la matrice complexe impliquant les applications, les utilisateurs et les exigences de temps au sein des entreprises afin de répondre aux conflits d'accès à la bande passante avant même qu'ils n'aient eu lieu.

### Caractéristiques et avantages de Cyberoam : QoS des applications

- Identifie les applications et les utilisateurs
- Offre un contrôle application-utilisateur-temps-bande passante
- Assure un accès aux applications
- Fournit des gains de productivité
- Contrôle les coûts de bande passante
- Offre une sécurité du réseau et des données

Cyberoam permet aux entreprises de savoir qui accède à quelle application, à quel moment et quelle quantité de bande passante est utilisée. En optimisant ainsi la consommation de bande passante, il offre des niveaux de productivité élevés et permet de maîtriser les coûts engendrés par cette dernière.

Non seulement Cyberoam prend en compte la sécurité des entreprises, mais également la productivité. Ainsi, il offre une solution efficace qui répond à tous les besoins des entreprises, et les prépare au Cloud.

## Éventail de sécurité de Cyberoam

 <p><b>Unified Threat Management (UTM)</b></p>	 <p><b>Cyberoam Central Console (CCC)</b></p>	 <p><b>SSL VPN</b></p>	 <p><b>Cyberoam iView</b> Journalisation et reporting intelligent</p>	<p>Protection des données &amp; chiffrement</p> <p>Contrôle des applications</p> <p>Gestion des périphériques</p> <p>Gestion du parc</p> <p><b>Cyberoam Endpoint Data Protection</b></p>
---	--	---	---	--

## Récompenses et certifications de Cyberoam



### Distributeurs Nationaux

**Afina:** +33 (0)141912314 | commercial@afina.fr  
**Config France:** +33158704010 | sales@config.fr  
**Eliptec Sas:** +33(0)383614440 | info@eliptec.com

Copyright© 1999-2011 Elitecore Technologies Pvt. Ltd. Tous droits réservés. Cyberoam et le logo de Cyberoam sont des marques déposées d'Elitecore Technologies Ltd. ©/TM. Marques déposées d'Elitecore Technologies ou des propriétaires respectifs des produits/technologies.  
 Bien qu'Elitecore s'efforce de fournir des informations précises, la société décline toute responsabilité relative à l'exactitude ou à l'exhaustivité de ces dernières. Elitecore se réserve le droit de changer, modifier, transférer ou réviser la publication sans préavis.

