Solutions pour Opérateurs Telecom

Les défis des Operateurs Telecom

Les opportunités de revenu et de services qui résultent de la transition des opérateurs télécom en fournisseurs de services IP, qu'ils soient fixes, mobiles, câbles (Opérateurs Multi Systèmes) ou revendeurs grossistes sont irréfutables. La migration des modèles de tarification à la minute vers des services basés sur des applications permet aux fournisseurs d'augmenter leur valeur, tout en tirant parti des avantages du déploiement rapide de ces nouveaux services. Les services de VoIP, de collaboration instantanée, de vidéoconférence et la mobilité sont désormais les vecteurs principaux de revenus pour les opérateurs. Les nouvelles architectures de cœur de réseau telles que IMS et LTE ont été conçues pour permettre aux opérateurs d'apporter la flexibilité et les améliorations opérationnelles nécessaires pour fournir ces services. En même temps, les opérateurs sont maintenant confrontés aux défis d'évolution. Dans le passé, les opérateurs télécom étaient considérés pour leur sécurité et pour leur fiabilité à 99,999%. L'architecture des PSTN/ RTCP (réseaux téléphoniques commutés publics), était fermée et pour la plus grande partie propriétaire, contrairement aux systèmes actuels sur IP où la sécurité pour des services temps réel comme la VoIP n'est pas intrinsèque et doit être envisagée avec des solutions dédiées.

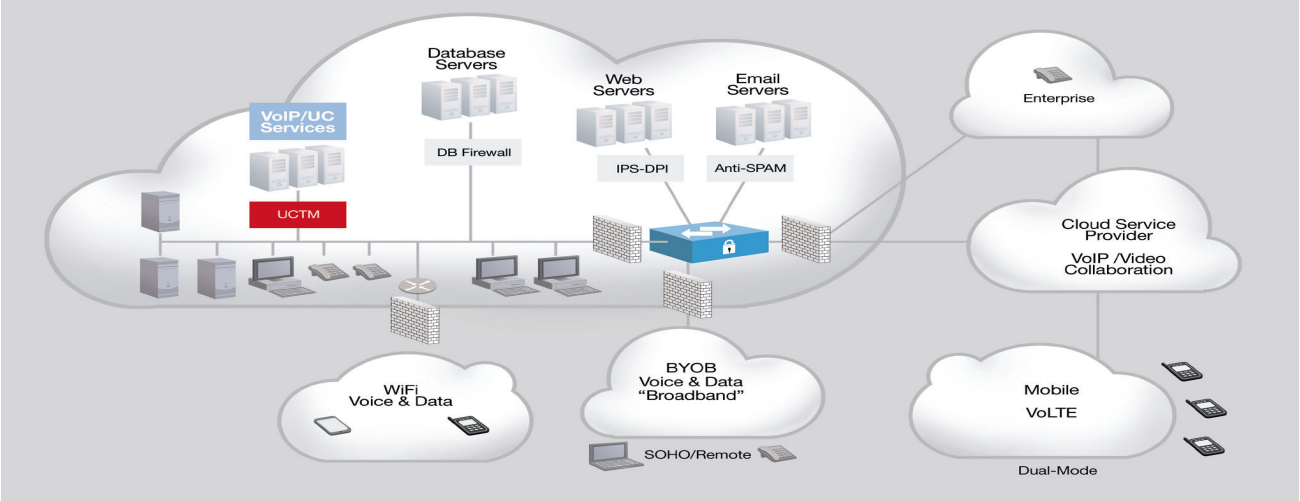

Figure 1: Protection des services VoIP dans les réseaux des Opérateurs

Les besoins des Opérateurs Telecom

Les clients s'attendent à ce que leurs services de communications soient sécurisés et comptent sur les fournisseurs de services pour assurer la sécurité du réseau et de ses composants de bout en bout. La gestion de la sécurité sur les réseaux VoIP est souvent abordée après leur mise en œuvre. Les implémentations des systèmes VoIP semblent se faire sur mesure à, partir de besoins spécifiques clients et sur des impératifs de revenu attendu. En même temps, les operateurs sont de plus en plus confrontés à un nombre croissant de vulnérabilités et susceptibles d être attaquées, tant en quantité qu'en sévérité, car les Communications Unifiées concentrées dans les réseaux des opérateurs deviennent des cibles de haute valeur pour les cyber criminels.

Les cybers criminels organisés et les hackers malveillants ciblent traditionnellement les services de data et les applications. Cependant, un nombre croissant de menaces émerge qui cible spécifiquement les différents composants des services VoIP comme les terminaux des utilisateurs, les Soft-Switch, les IP-PBX, les services SIP, les annuaires de réseaux (Type AD,LDAP radius) et bases de données utilisateurs. Le nombre et la fréquence de ces menaces sur la VoIP, et plus généralement sur les Communications unifiées (UC) ainsi que les pertes qui en résultent, obligent aujourd'hui les operateurs à repenser la protection de leurs réseaux. Attendre plus encore pour équiper les réseaux de ces nouveaux composants de sécurité, en faisant potentiellement face à des pertes conséquentes de revenus ainsi qu'à l'érosion de la confiance et de la loyauté des clients, serait catastrophique.

La fraude de taxation (Toll Fraud) et les attaques par Déni de Service (DoS/DDoS) prouvent l'existence de menaces significatives contre tous les operateurs. Hors, ces modèles d'attaques peuvent être détectés avec précision que par la mise en place d'une visibilité totale sur les actions des terminaux clients, les protocoles de signalisation et de médias, et la connaissance des applications SIP. Par la corrélation des différents évènements et avec une connaissance en profondeur des comportements des services, les pertes dues aux éléments logiciels compromis et aux utilisations non autorisées peuvent être rapidement évitées en réduisant les faux positifs qui se produisent quand les dispositifs de sécurité ont seulement une vue limitée du réseau et de son opération.
.

Une solution complète de détection, de visibilité temps réel, de gestion et de contrôle est indispensables pour sécuriser les composants essentiels du réseau d'un opérateur Telecom et devra assurer aussi bien la sécurité dans le cœur de réseau qu'aux extrémités et traiter les comportements, le trafic, la signalisation, les statuts d'appel, et la sécurité des terminaux ou logiciels clients.

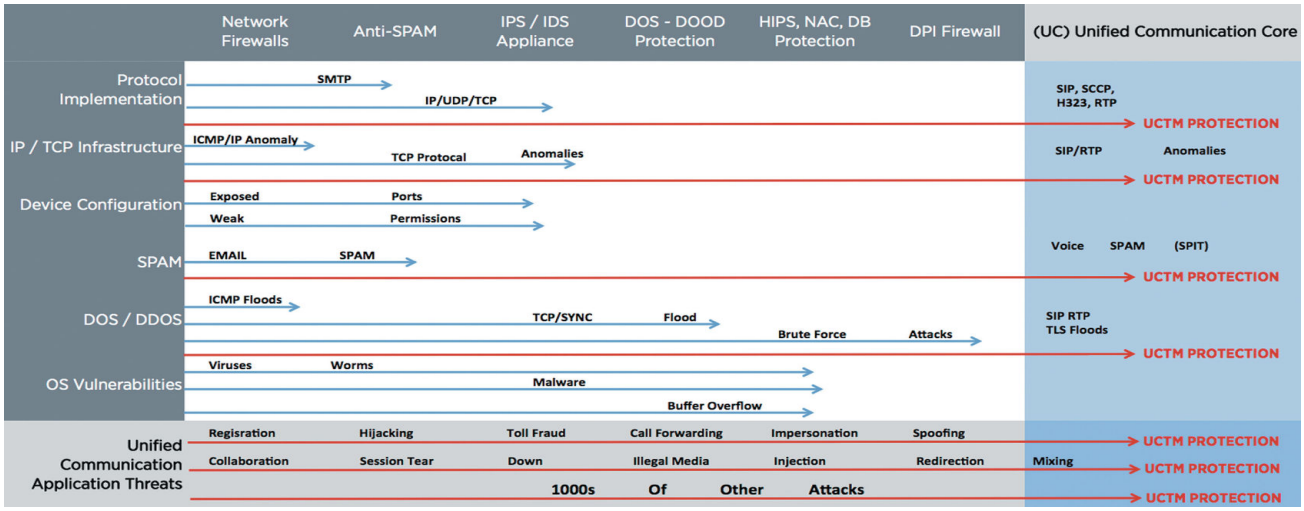

Figure 2: La Gestion des Menaces sur les Communications Unifiées – La VoIP crée de nouveaux besoins de sécurité.

RedShift Networks : des solutions pour les Opérateurs Telecom

- Offre la visibilité, le contrôle et la protection des éléments clés tels que Soft-Switch, les serveurs d'applications et les annuaires
- Permet la surveillance et analyse du trafic VoIP & UC
- Assure la sécurisation au niveau signalisation, medias et couches applicatives – couches 3 à 7, grâce à une fonction DPI.
- Dispose d'algorithmes d'apprentissage de comportement avancé
- Connaissance des différentes applications de Communications Unifiées et Collaboration
- Détection, prévention, remédiation et reporting sur les attaques.

La solution UCTM de RedShift Networks pour le cœur d'infrastructure basée sur une Appliance, permet à la fois de surveiller et d'assurer la sécurité des éléments, et du trafic du réseau .

- Grâce à sa technologie brevetée Redshift Networks UCTM est capable de détecter et de prévenir un large spectre de menaces sur les réseaux SIP.
- La solution inclut plus de 40 000 signatures de menaces et un moteur d'apprentissage dynamique de comportements des utilisateurs, qui identifie et signale le trafic anormal en temps réel.
- L' analyse proactive et la mise en oeuvre de politiques de sécurité permet aux operateurs d'identifier et d'atténuer les menaces le plus rapidement possible tout en réduisant les faux positifs et les faux négatifs.
- Les opérateurs peuvent bénéficier de mises a jours fournies par le réseau mondial des dispositifs de détection de menaces de Redshift Networks, s'assurant de suivre l'évolution des attaques au niveau mondial et régional.
- Avec une gamme complète de produits qui va de la classe entreprise jusqu'à la gamme opérateur mondial, les fournisseurs de services peuvent déployer une solution de sécurité intégrée et complète pour les UC & C, d'un éditeur unique.

Redshift Networks UCTM fait tout cela sans pour autant sacrifier la performance et la productivité des employés. Les équipements de sécurité Redshift Networks fournissent un point d'intégration, de visibilité, de contrôle et de protection pour les applications de communications unifiées d'entreprise.

RedShift Networks – la gamme de produit "Hawk / Eagle / Falcon"

- Technologie de Sécurité sur Flux Synchrones ™
- Protégé par brevets
- Technologie d'inspection dynamique du flux temps réel
- Architecture propriétaire proactive d'évaluation de menace
- Analyse et apprentissage de comportement avancés (utilisateur et application)
- Architecture logicielle évolutive
- Architecture distribuée
- Fonctionnalités haute disponibilité pour les réseaux mondiaux, robustes de VoIP dans le Cloud (Hawk / Eagle)