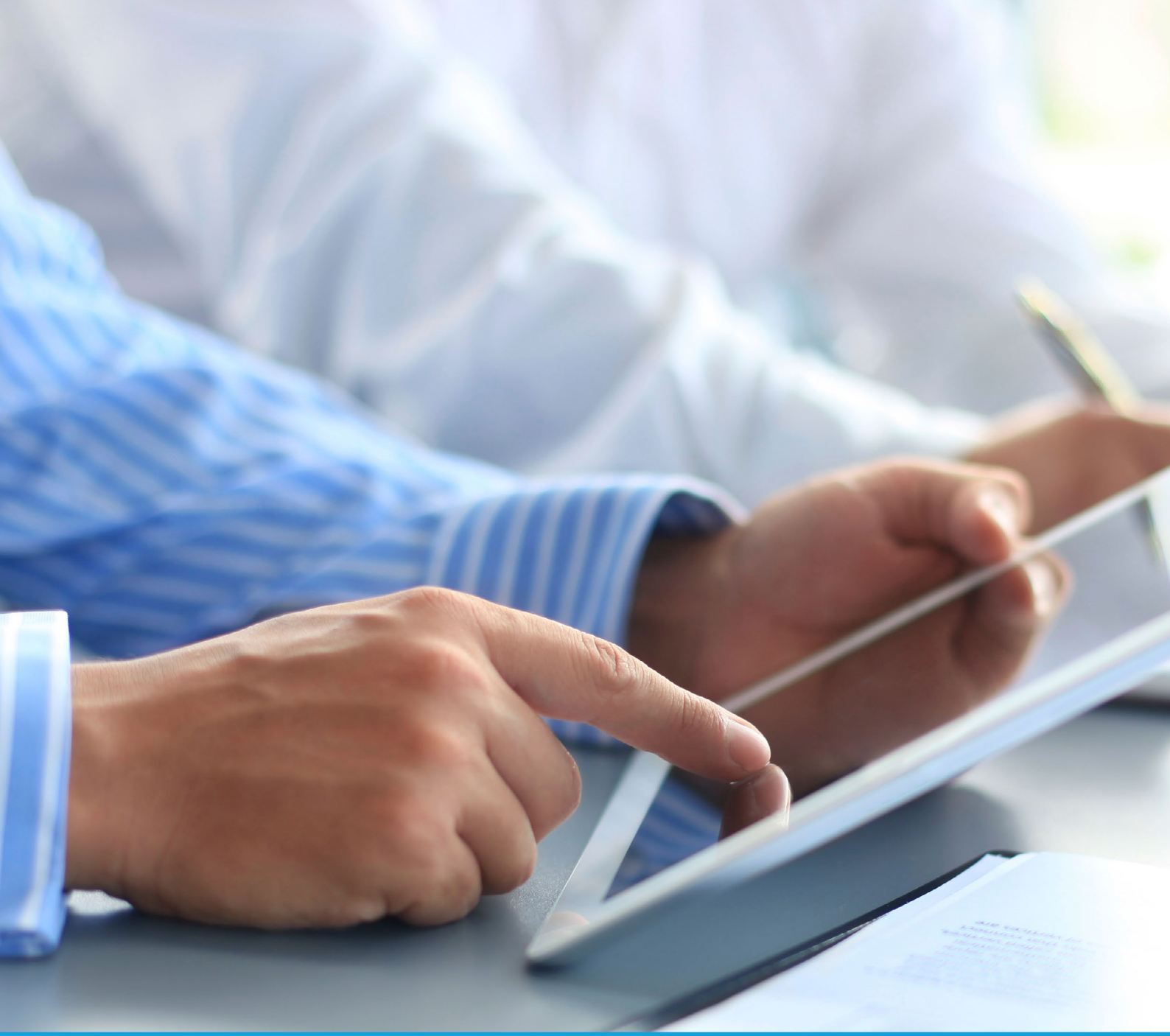
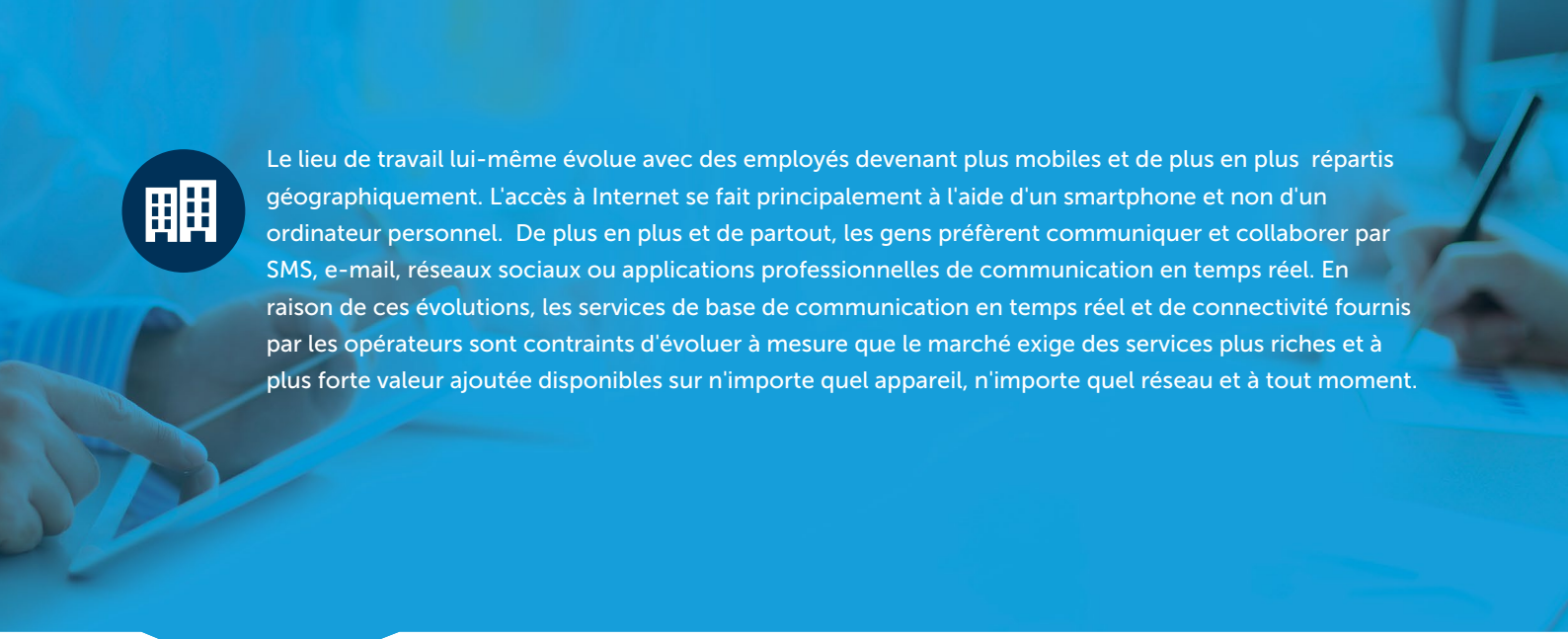


Sécuriser les Communications Mobiles en Temps Réel

Fournir un accès mobile sécurisé au cloud

Mitel
Powering connections

Un livre blanc Mitel



Le lieu de travail lui-même évolue avec des employés devenant plus mobiles et de plus en plus répartis géographiquement. L'accès à Internet se fait principalement à l'aide d'un smartphone et non d'un ordinateur personnel. De plus en plus et de partout, les gens préfèrent communiquer et collaborer par SMS, e-mail, réseaux sociaux ou applications professionnelles de communication en temps réel. En raison de ces évolutions, les services de base de communication en temps réel et de connectivité fournis par les opérateurs sont contraints d'évoluer à mesure que le marché exige des services plus riches et à plus forte valeur ajoutée disponibles sur n'importe quel appareil, n'importe quel réseau et à tout moment.

Avec les nombreuses possibilités offertes par les réseaux LTE et Internet pour améliorer les communications et la collaboration, la mise en œuvre de politiques et mesures de sécurité est devenue un élément important de l'équation. Pour beaucoup d'entreprises, tous les efforts réalisés en matière de sécurité ne sont pas suffisants ou ne peuvent pas être seulement en cours de réflexion. À mesure que les smartphones évoluent pour devenir principalement des plates-formes informatiques mobiles, ces appareils sont soumis aux menaces de sécurité qui évoluent également. Les opérateurs déplaçant désormais leur infrastructure de service dans le cloud, les entreprises sont de plus en plus préoccupées par la séparation et la confidentialité du trafic. Rares sont les offres du marché qui répondent de manière adéquate aux exigences d'une activité en constante évolution tout en maximisant la sécurité, la protection et l'accessibilité.

Évolutions du marché

De multiples évolutions interviennent dans le domaine des communications professionnelles mobiles. Alors qu'un changement des moyens de communication a eu lieu, il n'y a pas encore eu de substitution ou de remplacement généralisé d'un moyen par un autre. Au lieu de cela, les les nouvelles manières et moyens de communication et de collaboration augmentent et viennent compléter les modes de communication traditionnels vocaux et e-mail.

De plus en plus, les réseaux construits par les opérateurs mobiles sont, et seront, installés dans le cloud. Les opérateurs mobiles de niveau 1 actuels offrent déjà des services de communication en temps réel à forte valeur ajoutée à travers une infrastructure virtuelle. Le passage au cloud et aux architectures basées sur la virtualisation des fonctions réseau (NFV) présente des défis supplémentaires, parmi lesquels la séparation, la mutualisation, la sécurité et la confidentialité du trafic et l'orchestration, l'activation et la gestion du service.

Les évolutions principales du marché comprennent :

1. *L'augmentation des communications mobiles en tant que moyen principal et privilégié ;*
2. *La croissance (et la diversité) des options de communication non vocales en temps réel[1] ;*
3. *L'adoption accrue des politiques BYOD (Bring Your Own Device) dans le milieu professionnel ;*
4. *Le désir des consommateurs de bénéficier de services capables de se synchroniser sur différents appareils (ex. : smartphone, tablette et ordinateur) ;*
5. *La pression incitant à maximiser la productivité de l'entreprise et l'utilisation d'applications téléchargées individuellement dans l'environnement professionnel devancent la mise en place de politiques et de procédures appropriées par les services informatiques ;*
6. *La disponibilité et l'utilisation croissantes du Wi-Fi en tant que solution de mobilité principale des services (incluant les appels et la messagerie par Wi-Fi) sur le lieu de travail, chez soi et en déplacement ;*
7. *Le passage aux services fournis via le cloud à la fois pour les entreprises et les opérateurs de réseaux mobiles ;*
8. *Les menaces de sécurité devenant plus variées et sophistiquées. Les appareils mobiles sont de plus en plus soumis aux piratages informatiques et aux attaques.*

1. Par exemple, la communication et la collaboration par flux de travail et messagerie.

Présentation des défis et du problème

Les entreprises (et les opérateurs mobiles qui les fournissent) doivent contrebalancer les méthodes de communication dynamiques, imprévisibles et souvent non sécurisées par des mesures de sécurité et de contrôle. Les dirigeants d'entreprise souhaitent un cadre de travail qui permette au personnel de maximiser la productivité et l'efficacité, mais ont aussi besoin d'une solution qui garantisse une sécurité intégrale sur l'ensemble des environnements non sécurisés, non réglementés et non autorisés. Idéalement, la solution au problème est fournie sous la forme d'une solution logicielle sans investissement dans du matériel informatique spécialisé et qui permette l'autorisation, la gestion et la surveillance à distance, qui utilise des procédures et protocoles de sécurité standard (si possible), qui facilite les politiques BYOD et puisse être achetée en mode OPEX ou en mode CAPEX.

Réponse du marché et paysage concurrentiel

À ce jour, la sécurisation des communications en temps réel s'effectue au mieux entre le dispositif terminal et la périphérie du réseau mobile. Une fois que la demande de service traverse la périphérie pour atteindre le cœur du réseau, il n'y a aucune garantie quant au niveau de sécurisation des segments de liaison sur chaque partie de l'infrastructure de réseau interne[2].

Un nombre croissant d'applications alternatives[3] attirent les communautés d'utilisateurs qui sont davantage sensibilisées aux problèmes de sécurité. La communication point à point au moyen de la technologie WebRTC en plein essor nécessite le chiffrement des supports. Cependant, ces options sont généralement fournies à travers des communautés fermées, proposées au moyen d'approches non standard, sans interfonctionnement ou fédération et sont mises sur le marché telles quelles par le fournisseur de l'application.

Description de la solution

Mitel présente MiStealth, une offre élaborée par Unisys, qui fournit des services de communication en temps réel modernes et efficaces intégralement sécurisés. Les opérateurs de téléphonie mobile et les opérateurs de réseau mobile virtuel commercialisent cette solution en ciblant principalement les entreprises souhaitant un plus haut niveau de sécurité pour l'ensemble de leurs services mobiles. À titre d'exemple de solution permise par MiStealth, Mitel intègre une solution d'infrastructure mobile basée sur IMS permettant le VoLTE, VoWiFi et la messagerie avancée avec MiStealth.

2. 3GPP a des exigences de sécurité spécifiées pour les infrastructures de services, mais elles ne sont pas toutes entièrement mises en œuvre ou déployées. De plus, les spécifications sont à la disposition de tous ceux qui souhaitent les utiliser.
3. Jitsi (récemment acquise par Atlassian), Heml.is, RedFone, Secret, Signal, SilentCircle, TextSecure et Wickr.

Les communications en temps réel avec Mitel

La solution VoLTE/VoWiFi de Mitel comprend le cœur IMS (IMC), qui interagit avec les serveurs d'applications voix et de messagerie, le centre d'authentification, le service HSS (Home Subscriber Service) et le réseau à commutation de circuits à l'aide de la fonction de contrôle de media gateway. Il s'agit du composant principal de la solution IMS et tous les serveurs d'applications IMS interagissent avec celui-ci conformément aux spécifications 3GPP[4]. La solution IMS de Mitel comprend une gamme complète de fonctions de réseau de base décrites ci-dessous.

I-CSCF (Interrogating Call Session Control Function) : remplit les fonctions de localisation et de routage en interrogeant les services HSS pour obtenir des informations d'emplacement et d'inscription.

S-CSCF (Serving Call Session Control Function) : effectue les fonctions de contrôle de session, de contrôle de fonctionnalités/services, de service d'enregistrement, d'allocation des ressources et de routage.

CTAS (Converged Telephony Application Server) : le serveur CTAS de Mitel est un serveur d'application conforme aux normes IR.92/IR.94 qui fournit des services voix et vidéo sur les réseaux LTE. Le composant TAS de Mitel a été conçu spécialement avec de nombreuses fonctions standard offertes par un système mondial de communications mobiles (UMTS MSC) permettant ainsi à la solution d'appel VoLTE/Wi-Fi de Mitel de fournir une parité totale des services avec le réseau existant.

BGCF (Breakout Gateway Control Function) : sélectionne le réseau sur lequel un breakout (RTPC à commutation de circuits) doit avoir lieu et fournit des informations de routage.

SBC (Session Border Controller) : le composant SBC de Mitel est utilisé pour permettre l'accès sans fil à partir de réseaux Wi-Fi où la mobilité n'est pas requise ni prise en charge (sans quoi les appareils compatibles avec les appels Wi-Fi se connectent à la passerelle ePDG). Il prend également en charge la technologie VoLTE avec les fonctions eSR-VCC. Basée sur une architecture modulaire et flexible avec des plans de contrôle et multimédia pouvant évoluer indépendamment. La fonctionnalité SBC de Mitel est offerte en tant que composante de la passerelle UAG (Universal Access Gateway). De plus, la passerelle UAG offre des fonctions standard telles que l'ancrage multimédia, le transcodage, le transfert multimédia, le pare-feu et le contrôle d'accès. C'est le premier point de contact d'un terminal à capacité VoWiFi dans le réseau IMS. Pour une mobilité totale, la passerelle UAG peut également prendre en charge la fonction ePDG.

ePDG (Evolved Packet Data Gateway) : la passerelle ePDG est utilisée pour les réseaux d'accès Wi-Fi non sécurisés afin de fournir une tunnelisation IPSEC/IKEv2 et une amélioration des mécanismes d'authentification basée sur EAP du service d'appel Wi-Fi avec une mobilité totale en intégrant la passerelle ePDG comme un élément du réseau EPC. Les appareils compatibles VoLTE/VoWiFi traversent la passerelle ePDG pour se connecter de façon sécurisée au réseau et basculer de manière transparente entre les réseaux d'accès Wi-Fi et LTE sans interrompre les appels vocaux ou vidéo en cours.

MRF (Media Resource Function) : la fonction MRF est utilisée conjointement avec le CTAS pour diffuser des annonces. Elle interagit avec le CTAS sur le plan de contrôle et interagit avec la passerelle UAG pour le multimédia. La fonction MRF offre également les fonctionnalités multimédia requises pour les services de conférence téléphonique et de vidéoconférence, ainsi que d'autres fonctions de transcodage multimédia plus complexes pour des services plus avancés.

RMS (Rich Messaging Service) : le service RMS de Mitel est la plate-forme de messagerie IP de nouvelle génération prenant en charge les SMS avec les fonctions IMS ou l'interfonctionnement OMA CPIM sur les services SMS/MMS existants. Le service RMS assure une interconnexion avec le centre SMSC et gère l'envoi de SMS vers/depuis l'abonné mobile lorsqu'il est enregistré dans l'IMS. Le RMS est un composant du serveur d'applications IMS fournissant des services SMS avec IP pour tous les abonnés VoWiFi lorsqu'il y a une couverture Wi-Fi et connecte les abonnés VoWiFi au centre SMSC existant pour envoyer et recevoir des messages SMS.

Passerelle d'application (AG, Application Gateway) : la passerelle AG de Mitel remplit la fonction de passerelle de sécurité pour le trafic basé sur HTTP transmis de l'Internet public au réseau sécurisé de l'opérateur, laquelle est nécessaire à l'authentification et à l'autorisation du trafic HTTP lors de l'utilisation du service d'appel en Wi-Fi. La fonction de la passerelle AG est notamment couramment utilisée pour les services supplémentaires de changement d'utilisateur sur l'interface 3GPP Ut. La passerelle AG autorise la demande et permet une gestion de service supplémentaire en accès Wi-Fi.

PGW (Packet Data Network Gateway) : la passerelle PGW effectue le transfert de porteuse (Interface S2b avec la passerelle ePDG). La passerelle PGW prend également en charge l'ancrage de la mobilité IP entre les réseaux d'accès LTE et Wi-Fi. Elle peut être combinée en option avec le SBC d'accès dans une architecture convergente optimisée.

Client mobile : le client mobile VoWiFi de Mitel se conforme aux normes 3GPP et IETF ainsi qu'aux dispositions applicables de la norme GSMA IR.92. Le client est téléchargé sur le terminal et interagit avec les composants du combiné pour s'accrocher à une connexion Wi-Fi et s'enregistrer sur les serveurs d'applications Mitel. Une fois enregistré, le client VoWiFi de Mitel fonctionne parfaitement pour offrir des services de messagerie et d'appel vocal sur IP à l'utilisateur final.

CCPS (Client Configuration and Provisioning Server) : le serveur CCPS automatise le provisionning et la configuration en fonction de l'architecture d'auto-configuration RCS. Il s'appuie sur les demandes HTTP du client à un serveur dédié qui gère les données de configuration et interagit avec les plates-formes réseaux et informatiques du client pour authentifier et contrôler le comportement du client.

Passerelle de provisionning (PG, Provisioning Gateway) : la passerelle PG assure la parité des services CS et la synchronisation de la configuration des abonnés VoWiFi lors de l'enregistrement initial. Les mises à jour de service permanentes sont également prises en charge dans le domaine d'accès d'où proviennent les mises à jour. Cela comprend les changements introduits par l'intermédiaire du système de provisionning principal. Le fonctionnement de la passerelle PG est transparent pour l'utilisateur final.

IMS-HSS (IMS Home Subscriber Service) : le service IMS-HSS fournit le service HSS conformément à la norme IMS 3GPP et offre une interface standard 3GPP aux serveurs d'applications et au cœur IMS pour permettre des échanges de profils d'abonnés et d'autres fonctions.

Serveur d'application de messagerie vocale (VM AS, Voicemail Application Server) et mStore : le serveur VM AS associé à mStore offre des fonctions de dépôt et de notification des messages vocaux dans la solution lorsque l'abonné n'est pas joignable, est occupé ou déconnecté, etc.

4. Le cœur IMS est aussi désigné indifféremment « CSCF ».

MiStealth | Sécurité

La solution MiStealth s'intègre au portefeuille de produits Mitel pour les opérateurs et les entreprises.

MiStealth est une structure architecturale de sécurité offrant les avantages suivants :

1. *Segmentation du réseau IP en fonction de l'identité de l'utilisateur*
2. *Possibilité pour les extrémités du réseau de « se cacher », c'est-à-dire de devenir presque indétectables, sauf pour les utilisateurs autorisés*
3. *Sécurisation des données en mouvement grâce au chiffrement AES-256 reposant sur des clés éphémères avec une confidentialité persistante*
4. *Diminution de la dépendance à l'infrastructure physique pour plus de sécurité, permettant de renforcer les réseaux physiques et la diminution des coûts*
5. *Réponse rapide aux besoins changeants des entreprises en permettant le contrôle des droits d'accès au réseau par l'intermédiaire de systèmes de gestion de l'identité couramment utilisés tels que Microsoft Active Directory*

Communautés d'intérêts sécurisées : sur un réseau sécurisé par MiStealth, les extrémités ne peuvent généralement pas communiquer à moins que les utilisateurs sur ces extrémités soient des membres de la même communauté d'intérêts. Chaque communauté d'intérêts est généralement associée à un groupe d'utilisateurs préalablement défini dans un système de gestion de l'identité. De cette manière, un réseau plat est segmenté de façon dynamique en réseaux virtuels, où la connectivité ou la visibilité au sein de chaque réseau virtuel est déterminée par les définitions de l'utilisateur et du groupe dans le système de gestion de l'identité.

Chaque communauté d'intérêts dispose d'une clé cryptographique associée, et chaque extrémité du réseau reçoit les clés de sa communauté d'intérêts de façon dynamique en présentant les identifiants d'utilisateur à un service d'autorisation MiStealth. Le service d'autorisation utilise un système de gestion de l'identité pour authentifier les identifiants d'utilisateur et pour déterminer la communauté d'intérêts que chaque utilisateur est autorisé à recevoir.

Protocole de communauté d'intérêts sécurisée (SCIP, Secure Community of Interest Protocol) : le protocole SCIP permet à deux extrémités de déterminer si elles partagent une communauté d'intérêts, sans que l'une ou l'autre extrémité n'ait besoin de révéler sa communauté d'intérêts. Le protocole SCIP permet également à deux extrémités d'obtenir une clé secrète partagée éphémère utilisée ensuite par le protocole IKE (Internet Key Exchange) pour établir un tunnel IPsec entre les extrémités. De plus, le protocole SCIP permet à deux extrémités de s'entendre sur le profil cryptographique le plus sécurisé qu'elles prennent toutes les deux en charge.

Les extrémités protégées par MiStealth sont « cachées ». Une extrémité n'acceptera pas ou ne transmettra pas tout paquet non chiffré à moins qu'elle soit spécifiquement configurée pour le faire. De la même manière, une extrémité ne répondra pas à une négociation SCIP provenant d'une autre extrémité, à moins que les deux extrémités aient une communauté d'intérêts commune.

Aucune modification importante de l'équipement réseau sous-jacent n'est nécessaire. De plus, aucune modification des applications exécutées au sein de cette structure n'est nécessaire. MiStealth protège automatiquement les extrémités et leur trafic réseau à l'aide de communautés d'intérêts et de filtres afin de limiter le trafic autorisé sur la base des politiques spécifiques au rôle ou à l'utilisateur.

L'intégralité de la structure MiStealth est gérée de manière centralisée, prenant en charge le groupement des licences de toute l'entreprise. Dans le cadre du système de gestion, une surveillance et un contrôle renforcés des extrémités sont pris en charge.

La solution MiStealth comprend les éléments clés ci-dessous :

Enterprise Manager (EM) : un ensemble de services centralisé et réparti permet aux administrateurs de créer et gérer différents éléments MiStealth tels que les communautés d'intérêts, les filtres et les rôles ; de provisionner et surveiller géographiquement les composants EM dispersés ; et d'autoriser, surveiller et accorder une licence aux utilisateurs de MiStealth. Les composants EM peuvent être déployés dans une configuration haute disponibilité.

- *Le portail Enterprise Management (EM Portal) est l'interface utilisateur des administrateurs. Il est composé d'un ensemble de portlets que les administrateurs utilisent pour configurer et gérer l'environnement MiStealth.*
- *Le cœur du système Enterprise Management (EM Core) contient la base de données des éléments MiStealth et de leurs attributs. Il contient également la logique d'entreprise permettant la mise en œuvre des fonctions présentées sur EM Portal, et constitue un référentiel d'audit pour tous les événements relatifs à MiStealth au sein de l'entreprise.*
- *Le service d'autorisation (AuthSvc) répartit les communautés d'intérêts et les filtres aux extrémités selon l'identité de l'utilisateur. Il sert également de point de contrôle, d'enregistrement et d'autorisation pour les extrémités actives. Chaque extrémité est provisionnée par une liste ordonnée de services d'autorisation (AuthSvcs), et avance dans la liste de manière séquentielle jusqu'à recevoir les communautés d'intérêts.*
- *Le service de licence (LicSvc) conserve un pool de licences de différents types (ex. : serveur, poste de travail, mobile), et les distribue aux services d'autorisation (AuthSvcs) sur demande. Un pool de licences central peut être partagé par l'ensemble de l'entreprise et peut suivre les fuseaux horaires de manière dynamique à mesure que la demande change de zone géographique.*
- *Le service de surveillance (MonSvc) relie les composants EM centraux et répartis.*

EM peut être déployé soit comme un ensemble de ces cinq composants ou comme un sous-ensemble distribué contenant les services AuthSvc, LicSvc et MonSvc. L'un des déploiements complets comprenant les 5 composants doit être installé quelque part dans l'entreprise. Ce déploiement complet est dénommé « serveur Enterprise Management » (EMSvr). Les déploiements à trois composants (services AuthSvc, LicSvc et MonSvc), dénommés « serveurs d'autorisation » (AuthSvrs), peuvent également être effectués dans toute l'entreprise pour la redondance ou la localisation.

Les composants EM peuvent être installés sur Windows Server 2008 R2 ou 2012 R2. EM est distribué sous la forme d'une seule image (.iso), qui peut être installée sur un serveur autonome ou virtuel.

EM génère des packages d'installation utilisés pour installer l'agent MiStealth aux extrémités. Les packages sont adaptés au système d'exploitation de l'extrémité, à la liste ordonnée des services AuthSvcs que l'extrémité doit utiliser et à d'autres paramètres.

Extrémités : chaque extrémité autorisée par MiStealth dispose d'un agent MiStealth. L'agent se charge de communiquer avec les services AuthSvcs pour autoriser les utilisateurs et obtenir les communautés d'intérêts, demander une licence et enregistrer les événements relatifs à MiStealth. L'agent manipule également les filtres du paquet du système d'exploitation d'origine pour rester « caché » sur le réseau, effectuer la négociation SCIP, établir les tunnels IPsec et autoriser ou refuser des flux de trafic spécifiques.

Les packages d'installation des extrémités peuvent être distribués à l'aide d'outils de distribution de logiciel courants, tels que Microsoft SCCM, et peuvent être installés silencieusement sans intervention de l'utilisateur.

MiStealth Secure Virtual Gateway (SSVG) : les systèmes d'exploitation pour lesquels il n'existe pas d'agent MiStealth d'origine disponible peuvent se connecter aux réseaux MiStealth en utilisant une passerelle SSVG. La passerelle SSVG est placée de façon topologique devant les systèmes à protéger, avec un segment de texte en clair entre ces systèmes et la passerelle SSVG aussi petit que possible. Au sein de la passerelle SSVG, chaque système protégé est configuré à l'aide des identifiants d'utilisateur. Les identifiants d'utilisateur déterminent, par l'intermédiaire de la méthode d'autorisation MiStealth, la communauté d'intérêts attribuée au système protégé.

De multiples systèmes contenant du texte en clair peuvent être protégés par une passerelle SSVG, chaque système avec ses propres identifiants d'utilisateur uniques.

La passerelle SSVG se présente sous la forme d'une image système Linux qui peut être installée sur un serveur physique dédié, ou sous la forme d'une machine virtuelle dans un environnement virtuel.

Secure Remote Access Gateway (SRA-GW) : les systèmes, les appareils ou les applications mobiles spécifiques ayant besoin de se connecter à un intranet protégé par MiStealth, mais qui sont en dehors de l'intranet, peuvent se connecter grâce à la passerelle SRA-GW.

Comme pour la passerelle SSVG, chaque extrémité distante est représentée comme une extrémité MiStealth unique à l'intérieur de l'intranet. Avec la passerelle SRA-GW, contrairement à la passerelle SSVG, les utilisateurs sont authentifiés de manière dynamique au lieu d'être configurés de manière statique, et la connexion de l'extrémité distante à la passerelle SRA-GW est un tunnel IPsec VPN hautement sécurisé.

Les extrémités distantes peuvent être des systèmes ou des appareils avec des capacités IPsec VPN d'origine ou des applications mobiles qui ont été « enveloppées » à l'aide de la protection d'application mobile Mocana.

La passerelle SRA-GW nécessite un composant supplémentaire, la passerelle IPsec VPN Gateway (VPN-GW) pour supprimer les tunnels IPsec depuis les extrémités distantes. La passerelle de sécurité MiStealth de Mitel joue le rôle de la passerelle VPN-GW.

Avantages de MiStealth

Communautés d'intérêts sécurisées : MiStealth parvient à segmenter le réseau de manière dynamique en utilisant SCIP, IKE et IPsec pour mettre en œuvre des communautés d'intérêts sécurisées reposant sur l'identité de l'utilisateur. Les extrémités sont cachées au trafic non autorisé.

Solution logicielle : aucun dispositif matériel n'est requis pour déployer un environnement compatible avec MiStealth. Tous les composants sont fournis sous la forme de logiciels et sont adaptés pour être exécutés dans des environnements virtuels ou sur un serveur physique dédié fourni par l'entreprise ou l'opérateur.

Octroi de licences d'entreprise : les licences MiStealth peuvent être partagées par l'ensemble de l'entreprise, ces dernières sont disponibles là où elles sont nécessaires, à la demande.

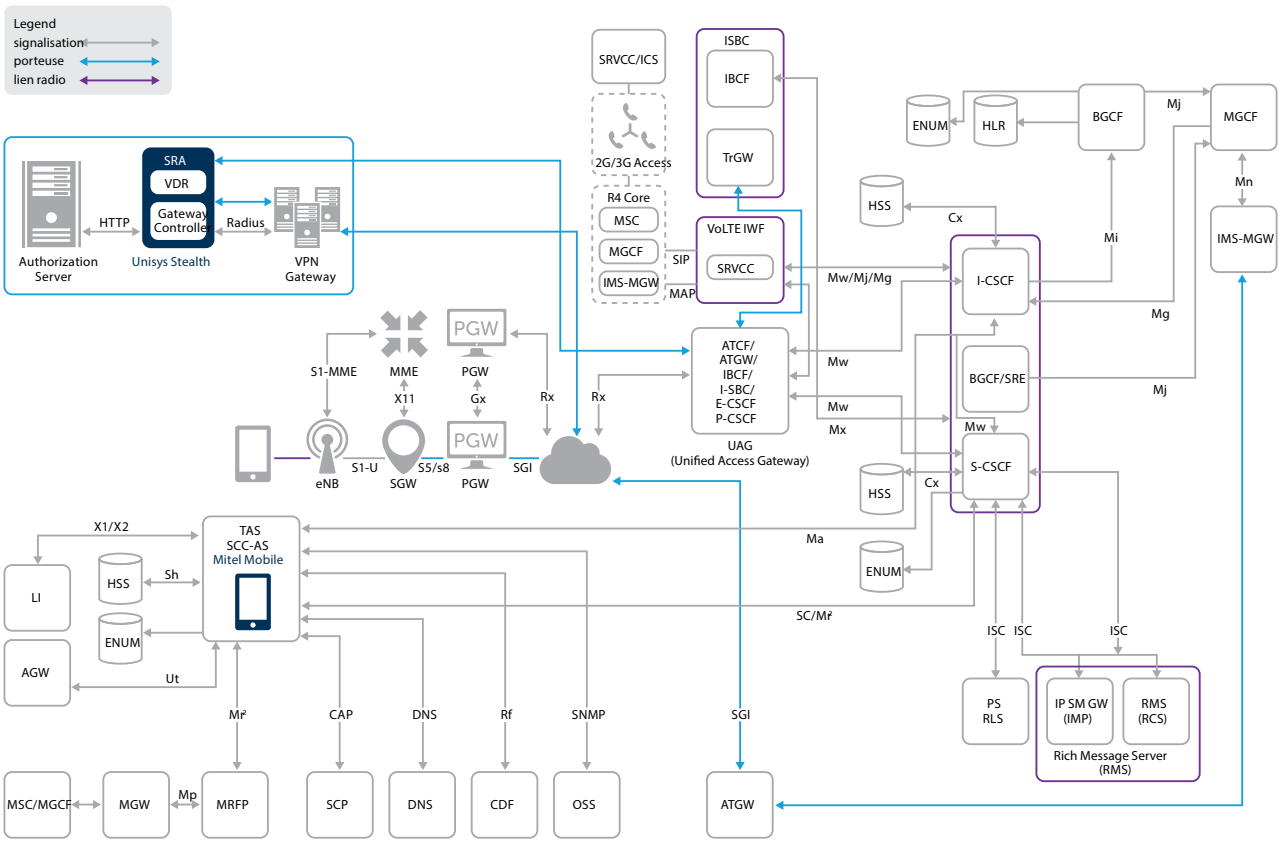
Exploitation des systèmes de gestion de l'identité : MiStealth permet de gérer l'accès réseau en fonction de groupes définis dans les systèmes de gestion de l'identité couramment utilisés tels que Microsoft Active Directory.

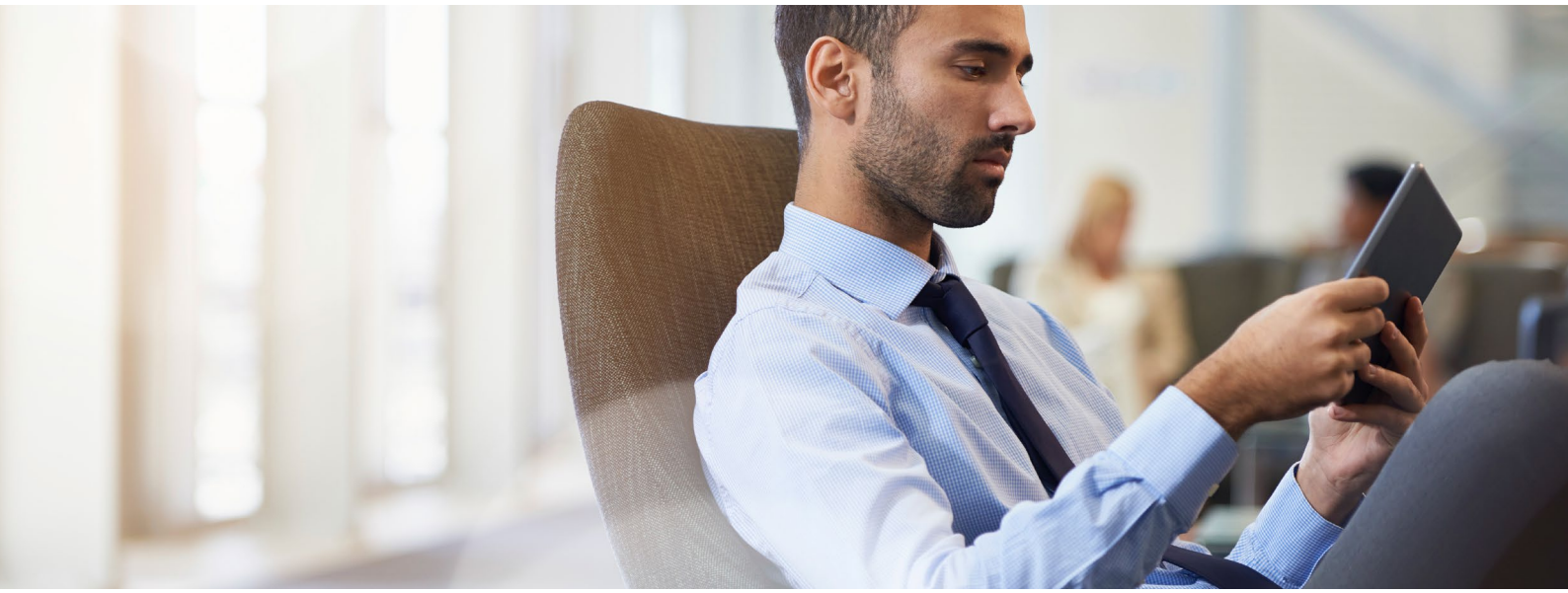
Protocoles et méthodes de sécurité standard : Internet Key Exchange (IKE) et IPSec sont les protocoles sous-jacents d'échange de clés, d'établissement de tunnels et de transfert de données. L'utilisation de ces protocoles standard améliore la performance des extrémités, permet une prise en charge plus étendue des plates-formes de système d'exploitation et facilite une adoption à plus grande échelle.

Gestion centralisée : la définition, le provisionning et la conservation de tous les éléments MiStealth, tels que les communautés d'intérêts, les rôles, les services d'autorisation et les packages d'installation d'extrémités sont centralisés à l'aide d'un portail Web qui peut être localisé n'importe où sur le réseau.

Aucune modification des applications ou des procédures utilisateur : MiStealth fonctionne automatiquement et ne nécessite pas de modification du code d'application. L'agent MiStealth obtient les clés de communautés d'intérêts automatiquement lorsqu'un utilisateur se connecte.

Vue holistique d'une solution de communications mobile en temps réel sécurisée





Différenciation de la solution

La solution Mitel est unique sur le marché en terme fonctionnalité et de proposition de valeur.

Sécurité intégrale

Les solutions mobiles fournies par les opérateurs de téléphonie mobile offrent généralement une sécurité entre l'extrémité et la périphérie du cœur du réseau. Dans un environnement IMS, le P-CSCF maintient l'association de sécurité entre l'extrémité et le cœur du réseau. Cependant, une fois à l'intérieur du cœur, il n'y a aucune garantie concernant la manière de sécuriser le trafic et le niveau de sécurisation. La solution MiStealth fournit une sécurité tout au long du réseau, d'une extrémité à l'autre.

Portabilité

La solution offre une structure permettant à une entreprise ou une organisation d'établir et de mettre en œuvre des politiques de sécurité associées à un utilisateur plutôt qu'à un terminal.

Itinérance

Les utilisateurs qui voyagent en dehors de la zone de couverture de l'opérateur bénéficient de la capacité de la solution à fournir une sécurité intégrale depuis l'application mobile à travers tous les segments que le service traverse.

Au-delà des communications en temps réel

Dans le cas où une entreprise ou une organisation souhaiterait inclure une gamme plus large d'applications mobiles (ex. : e-mail, CRM, ERP), l'opérateur MNO/MVNO peut élargir le champ d'application de la solution et fournir une valeur ajoutée à la solution.

Faire le bon choix

Les entreprises et les organisations doivent être prudentes lorsqu'elles prennent des décisions concernant les communications en temps réel. Elles doivent faire le meilleur choix pour s'adapter aux méthodes de communication souhaitées par leur personnel tout en assurant la sécurité. Les opérateurs mobiles doivent prendre en compte les préoccupations relatives à la sécurité de cette nouvelle gamme de services et apporter une réponse à la menace grandissante des failles de sécurité des communications mobiles. Les opérateurs de téléphonie mobile sont également déterminés à améliorer le revenu moyen par utilisateur et à concevoir des offres réellement différenciées. La solution de communications en temps réel MiStealth de Mitel répond pleinement à toutes ces attentes.

Contactez-nous aujourd'hui pour en savoir plus.

Mitel
Powering connections

mitel.fr

583194-R1604-FR