Chiffrement natif d'Alcatel-Lucent OmniPCX Enterprise Purple

Chiffrement logiciel des communications et plateforme renforcée contre les cyberattaques

La transformation numérique est maintenant une réalité pour la plupart des organisations (publiques et privées). Aujourd'hui, les employés peuvent collaborer en tout lieu, avec la possibilité de communiquer en temps réel. Mais tous les outils de communication ne fournissent pas le cadre nécessaire permettant de répondre à la **disponibilité continue**, **la sécurité**, **la confidentialité** et **la conformité**.

Alcatel-Lucent Enterprise (ALE) accompagne des entreprises et des clients du monde entier pour comprendre les nouveaux défis auxquels ils sont confrontés et pour proposer les **solutions de communications unifiées et sécurisées** qui permettent à leurs collaborateurs de travailler en tout lieu, avec n'importe quel appareil.

Ce document décrit comment **ALE protège vos communications contre les cyberattaques**, grâce à une plateforme de communication sécurisée depuis sa conception, ouverte au cloud avec une architecture hybride, des mécanismes de chiffrement natif de pointe, offrant ainsi un contrôle total à votre équipe informatique et une conformité avec vos politiques de sécurité et vos meilleures pratiques.

Alcatel·Lucent Enterprise

Le paysage actuel de la cybersécurité

Le passage à un environnement numérique a entraîné une augmentation rapide des attaques de phishing et par ransomware. Il s'agit d'une préoccupation sérieuse compte tenu du nombre croissant de télétravailleurs, et pour toutes les organisations (publiques et privées). Avec l'augmentation des cybermenaces, les entreprises doivent travailler plus que jamais pour protéger leurs collaborateurs et leurs clients.

Un aspect important est le fait que le passage au cloud entraîne l'augmentation de la « surface d'attaque », ce qui signifie que les pirates pourraient exploiter l'ouverture non sécurisée des services basés sur le cloud ou du Software as a Service (SaaS). L'équipe informatique se doit donc d'être extrêmement exigeante sur les niveaux de service (SLA) du fournisseur et des vendeurs.

Approche par ALE de la sécurité depuis la conception

Un examen complet du paysage actuel permet aux entreprises de déterminer les stratégies de protection nécessaires pour leur équipement informatique. Par exemple, ALE offre aux entreprises les solutions dont elles ont besoin pour se conformer aux réglementations nationales et internationales, telles que la conformité au règlement général sur la protection des données (RGPD), HDS ou HIPAA (pour le secteur de la santé), NIS2 pour la cybersécurité dans les pays de l'Union européenne.

ALE offre également une connectivité sécurisée dans le cloud, avec des éléments d'authentification mutuelle et de chiffrement, une meilleure confidentialité des communications lors des réunions, ainsi que le contrôle des données privées dans le cloud. Une solution complète et sécurisée, prenant en compte l'évolution de l'environnement des entreprises, permet aux équipes de travailler en confiance quel que soit le contexte.

La confidentialité et la fiabilité des services cloud sont parfois remises en question. Les services cloud d'ALE offrent une politique stricte de confidentialité des données avec des centres d'hébergement situés à différents endroits pour une couverture mondiale du service. ALE dispose de points de présence dans des pays soucieux du respect de la vie privée, comme la France, l'Allemagne, les États-Unis, le Canada, Singapour et l'Australie. De façon contractuelle, les données personnelles des utilisateurs ne sont pas utilisées à des fins commerciales ou de marketing, et ALE garantit la conformité aux réglementations locales en matière de confidentialité des données, telles que le RGPD dans les pays européens. Les services cloud d'ALE sont également certifiés ISO 27001 pour la gestion de la sécurité des systèmes d'information et certifiés CSPN par l'ANSSI en France.

Les services cloud d'ALE sont également en mesure de s'interconnecter avec les serveurs de communication du client. Il peut ainsi conserver son système de communications professionnelles sur site et le connecter au cloud afin de bénéficier d'applications et de services de collaboration innovants.

Architecture hybride pour les communications unifiées

La plateforme de collaboration et de communications unifiées constitue un outil important pour l'entreprise. Cependant, le retour sur investissement n'apparait réellement qu'avec l'adoption par l'ensemble des groupes de travail. Pour cela, toutes les parties prenantes de l'organisation doivent être consultées, leurs préoccupations prises en compte et traitées, notamment l'équipe informatique chargée des politiques de sécurité.

Trop souvent, les mesures de sécurité entravent l'utilisation régulière de nouveaux services innovants. Lorsqu'il s'agit de travail collaboratif, l'expérience utilisateur doit rester intuitive. Sur le plan administratif, il est important de vérifier la compatibilité des plateformes en fonction des environnements approuvés par le service informatique, y compris, par exemple, l'autorisation des applications mobiles pour les smartphones et tablettes, type Android et IOS. En outre, la solution collaborative et le serveur de communication doivent dialoguer par le biais d'API ouvertes afin de faciliter la gestion et le contrôle des services téléphoniques et des échanges en temps réel. Cette évolution conduit les équipes informatiques à effectuer davantage de contrôles en amont.

Alcatel-Lucent Enterprise fournit des solutions complètes de **communication et de collaboration dans le cloud** et **sur site** qui vont dans le sens de la transformation numérique des entreprises. Les solutions de communication d'ALE permettent la continuité des appels en tout lieu, dans n'importe quelle situation, et à partir de n'importe quel appareil.

Fonctionnalités clés de la solution ALE pour protéger les communications :

- **Connectivité sécurisée** entre le système de communication sur site (IP-PBX et téléphones) et l'infrastructure cloud, exploitée par ALE, avec authentification mutuelle, chiffrement et élément de sécurité en bordure (SBC) afin de sécuriser l'accès au réseau public
- **Connexion transparente** au sein de l'entreprise et à l'extérieur. L'infrastructure de communication sous-jacente connecte les employés à distance avec ceux qui travaillent dans les bureaux et les locaux, quel que soit leur appareil, assurant la compatibilité avec les technologies standards telles que l'analogique, le numérique, IP, SIP, la voix à travers le WIFI, DECT. Tout en fournissant à l'équipe informatique des données pour surveiller la qualité de service (QoS)
- **Haute disponibilité** atteignant 5x9 avec des architectures redondantes déployées sur le site du client ou hébergées dans un cloud privé, 100 % logiciel et entièrement virtualisé, avec une protection contre les attaques par déni de service (DoS), et des fonctions natives de sécurité au niveau des équipements physiques et des systèmes d'exploitation
- **Confidentialité et protection des données** avec un contrôle d'accès basé sur les rôles et le chiffrement des données stockées. Cela permet de garantir que toutes les données cruciales sont entièrement protégées de bout en bout et sous votre contrôle.
- **Confidentialité des communications** : des mécanismes de chiffrement puissants, respectant les normes du secteur, mises en œuvre de façon native dans la solution, sans aucun impact sur la qualité et les performances vocales, fournissant l'expérience attendue par les clients et les employés

Les communications sont susceptibles d'être interceptées et écoutées par quiconque, sur le réseau de l'entreprise (LAN ou WLAN) et encore plus sur Internet. De nombreuses contre-mesures au niveau de l'infrastructure du réseau minimisent le risque d'interception (environnement LAN commuté, segmentation VLAN, gestion des ACL entre VLAN, protection ARP contre l'usurpation d'identité ou les attaques de type "flooding"), mais la seule façon d'assurer une protection complète est de faire en sorte que la conversation soit entièrement chiffrée en transit : même en cas d'interception par une personne malveillante, la conversation vocale restera inaudible car le déchiffrement est impossible.

La solution OmniPCX® Enterprise Purple (OXE Purple) par Alcatel-Lucent Enterprise fournit un **chiffrement natif** intégré afin d'assurer un chiffrement complet pour toutes les communications sur le réseau (Internet et privé).

Principes du chiffrement natif d'OXE Purple

OXE Purple offre une solution de communication professionnelle adaptée à l'ère numérique. Il connecte l'intégralité de l'entreprise et offre aux organisations la **liberté**, l'**agilité** et la **sécurité** pour développer leurs activités en toute confiance.

OXE Purple offre :

- La **liberté** d'être connecté à tout moment avec les clients et les collaborateurs. Au bureau, dans un batiment, en déplacement ou en télétravail. Depuis un smartphone, un ordinateur ou un téléphone dédié.
- L'**agilité** pour automatiser la gestion des communications professionnelles au sein d'un cloud privé et pour intégrer les interactions temps réel dans les processus métiers.
- La **sécurité** pour toutes les interactions au sein de l'entreprise et à l'extérieur, qu'il s'agisse d'une conversation avec un collègue, un partenaire, un client ou un agent du centre de contact. Au téléphone, sur une application de l'ordinateur ou d'un smartphone, en visioconférence et depuis une messagerie instantanée sécurisée dans le cloud.

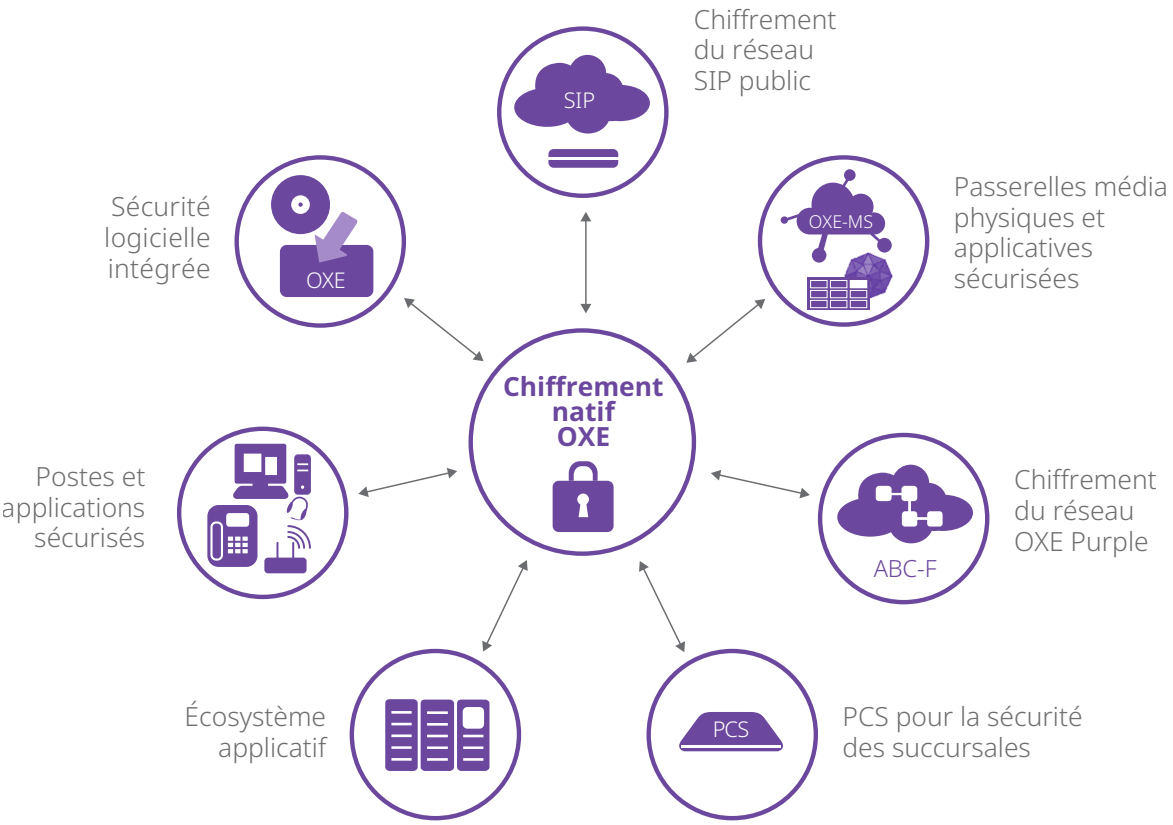
Cette technologie peut être déployée en toute sécurité dans n'importe quel environnement : sur site ou hébergée dans un cloud privé. C'est une solution **100 % logicielle** qui prend en charge la **virtualisation** et offre une **haute disponibilité 5x9** avec une redondance à chaud des composants principaux.

Elle assure la confidentialité grâce à des normes de chiffrement de pointe, avec le chiffrement intégral de toutes les conversations, quel que soit le dispositif ou l'application logicielle. Elle s'appuie sur une architecture flexible, qui lui permet de cibler les utilisateurs sensibles parmi tous les employés utilisant des appareils IP ou non IP.

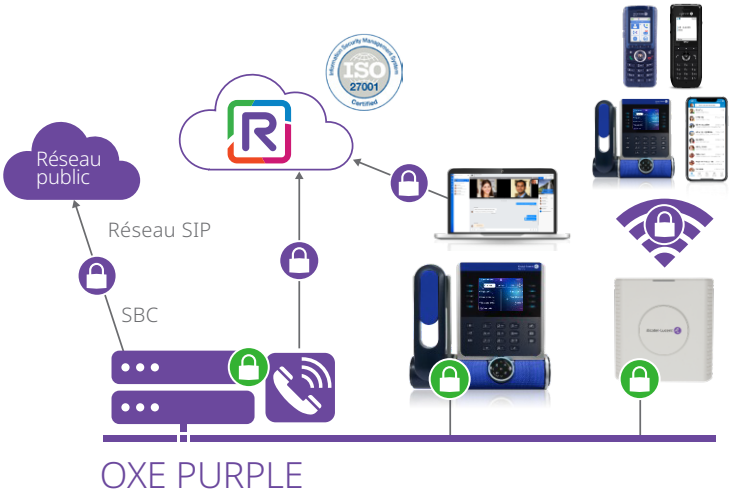
Composants du chiffrement natif d'OXE Purple

Le chiffrement natif d'OXE Purple offre :

- Le **chiffrement des flux de signalisation** à l'aide du protocole DTLS (Datagram Transport Layer Security). Ceci s'applique aux flux de signalisation échangés entre le serveur de communication OXE Purple et les postes téléphoniques IP ainsi que les applications compatibles DTLS.
- Le **chiffrement des flux vocaux** à l'aide du protocole SRTP. Cela s'applique aux flux vocaux échangés entre les postes et les applications compatibles DTLS.
- Les **connexions DTLS** (pour le chiffrement de la signalisation) établies avec une authentification du serveur ou une authentification mutuelle (serveur et client).
- Des **passerelles multimédias IP sécurisées** (basées sur un matériel propriétaire ou purement logicielles) pour le traitement chiffré du média voix, notamment les téléphones non IP connectés à des cartes matérielles (numériques et analogiques).
- Le **chiffrement des communications** vers le réseau public par faisceau SIP jusqu'à l'élément de bordure réseau du fournisseur de services en utilisant SIP TLS.
- Le **chiffrement des conversations** à l'aide de l'application client Rainbow (sur l'ordinateur, web, smartphone Android et iOS) par le biais de la passerelle Rainbow WebRTC pour les communications internes (vers un poste ou une autre application gérée par le serveur de communication OXE Purple) ou vers le réseau public.
- Le **chiffrement des communications** dans un réseau de serveurs de communication OXE Purple.
- La **prise en charge de la géo-redondance** du serveur de communication OXE Purple et du Passive Communication Server (PCS) pour les succursales sécurisées en mode survivabilité.
- L'**autorité de certification (CA) et le Trust Store intégrés** pour une authentification basée sur des certificats avec la possibilité pour le client de personnaliser le certificat avec une infrastructure clé publique (PKI) externe pour une confidentialité totale.



Le chiffrement natif d'OXE Purple prend en charge la plupart des appareils et applications IP connectés au serveur de communication (y compris les téléphones de bureau, les combinés mobiles DECT et les softphones). Il prend également en charge le chiffrement complet en transit pour un utilisateur équipé d'un matériel non IP (par exemple un téléphone analogique ou numérique) connecté à une passerelle multimédia matérielle gérée par le serveur de communication OXE Purple. En outre, la fonction prend en charge l'application collaborative basée sur le cloud Rainbow™ d'Alcatel-Lucent Enterprise.

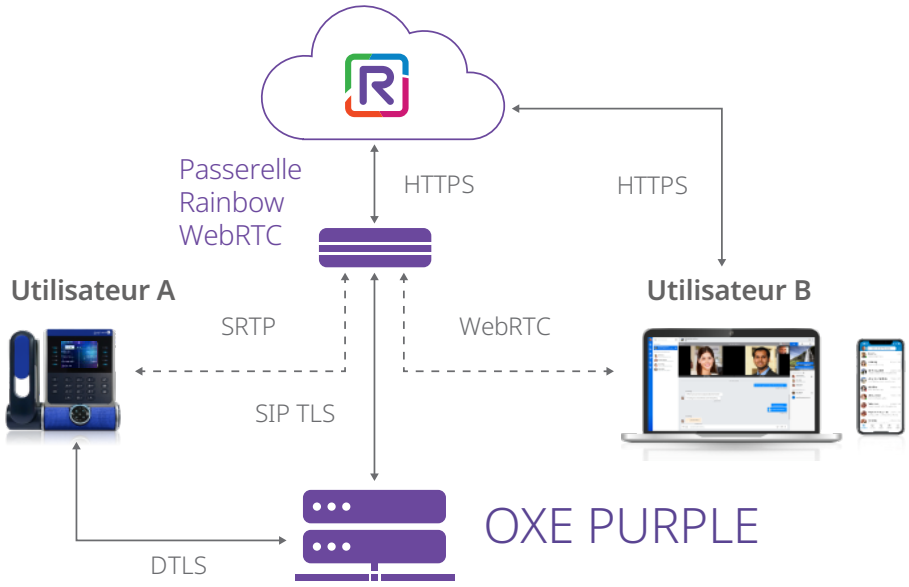


La connexion entre le serveur de communication OXE Purple et les services cloud de Rainbow est assurée par le composant logiciel de la passerelle Rainbow WebRTC.

La passerelle Rainbow WebRTC génère une paire de clés asymétriques et exporte une demande de signature de certificat (CSR) à signer par une autorité de certification (CA) qui peut être l'autorité de certification intégrée au serveur de communication OXE Purple ou une infrastructure clé publique (PKI) externe. L'identité de la passerelle Rainbow WebRTC est contrôlée par le serveur de communication OXE Purple pendant la phase de handshake TLS à l'aide de la liste de certificats de confiance (CTL) dans son Trust Store.

Comme illustré dans le diagramme ci-dessous, le média voix est chiffré en transit entre l'utilisateur A sur un téléphone de bureau et l'utilisateur B doté de l'application client Rainbow, sur PC/Mac/Web ou smartphone. La passerelle Rainbow WebRTC assure le relais en temps réel du flux SRTP entre l'utilisateur A et l'utilisateur B.

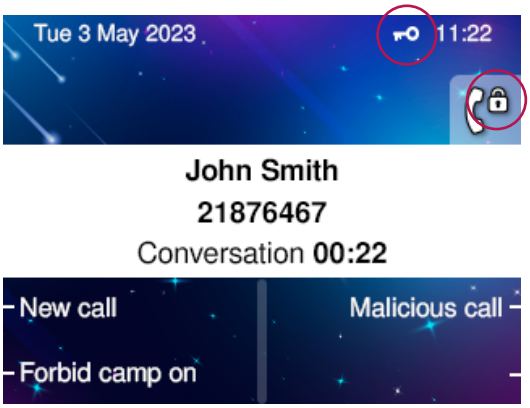
La passerelle Rainbow WebRTC est un composant 100% logiciel virtualisé qui prend en charge la duplication et la répartition de la charge pour une meilleure évolutivité.



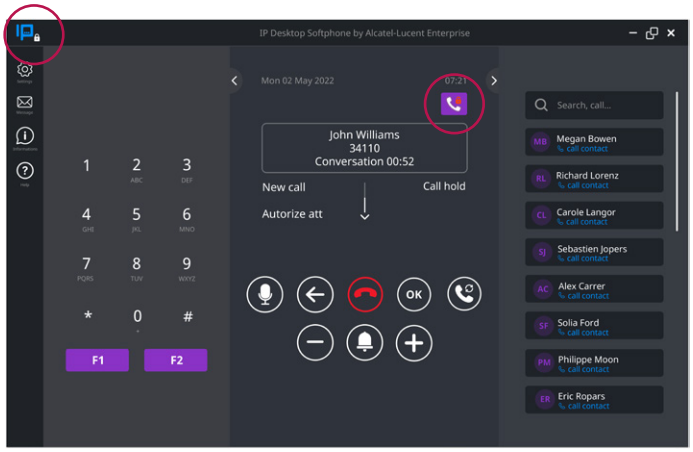
Icône de chiffrement sur les téléphones et les applications de softphonie ALE

Lorsqu'une communication est chiffrée, une icône en forme de cadenas ou de bouclier apparaît sur l'écran du téléphone ou dans l'application de softphonie. Ce mécanisme permet aux utilisateurs d'avoir confiance dans la confidentialité de la conversation.

ALE DeskPhones



Softphonie



IP Desktop Softphone

Caractéristiques et avantages

Fonctionnalités	Avantages
Confidentialité client/équipement (protocole de signalisation et média)	Empêche les attaques malveillantes, l'usurpation de téléphones IP et l'écoute des communications
Authentification mutuelle et intégrité de la signalisation pour la gestion des appels (assurant que les messages n'ont pas été modifiés)	Protection des communications professionnelles contre les attaques par déni de service
Prise en charge de DTLS 1.2 avec AES 256 et SRTP avec AES 128 : • 100 % solution logicielle • Authentification par certificat SHA2 4096 bits • ALE Enterprise et Essential DeskPhones (IP), IP Desktop Softphone, compatibles avec les postes ALE Premium série S • GD4-XL / GD4/GD3/INTIP3/OMS et PCS • Chiffrement IP-XBS DECT	Mécanismes de chiffrement de pointe pour garantir le plus haut niveau de protection et de confidentialité pour toutes les conversations, quel que soit le dispositif matériel ou l'application logicielle utilisé par l'employé
Prise en charge de TLS 1.2 avec AES 256 et SRTP avec AES 128 : • ALE Enterprise DeskPhones en mode SIP, ALE-2 et ALE-3, ALE SoftPhone • Réseaux SIP • Chiffrement de la passerelle Rainbow WebRTC	Protection des conversations au sein du réseau de l'entreprise et à l'extérieur, notamment l'accès au réseau public à l'aide de faisceaux SIP
Icône de chiffrement sur le téléphone et dans l'application softphone pour indiquer que l'appel est chiffré et sécurisé	Confiance de l'utilisateur final dans la confidentialité de la conversation
Chiffrement des appels en transit avec l'application Rainbow via la passerelle WebRTC	Garantie de la confidentialité des conversations des employés utilisant l'application client Rainbow sur PC/Mac, Web, smartphone Android et iPhone
Chiffrement de l'enregistrement des appels avec Alcatel-Lucent OmniPCX® RECORD Suite	Garantie de la confidentialité des conversations enregistrées
Fonction de chiffrement logiciel intégré dans la solution OmniPCX Enterprise Purple	Mise en œuvre simple sans gestion complexe au niveau du système de communication pour un niveau de sécurité optimal
Aucun impact sur les paramètres de qualité de service (QoS) et la configuration du réseau	Déploiement et configuration simples, sans qu'il ne soit nécessaire de modifier l'infrastructure de réseau
Prise en charge de la redondance géographique et de la survivabilité pour les succursales locales	Continuité des activités dans toutes les situations sans compromettre la confidentialité en cas de défaillance du réseau, du serveur ou du centre de données

Recommandations et bonnes pratiques d'ALE

Tous les organismes (publics et privés) représentent des cibles potentielles pour les cyberattaques. Il est donc essentiel de mettre en œuvre un système de communication le plus sûr possible. Les outils de gestion intégrés doivent permettre de superviser la sécurité de tous les éléments.

En outre, les appareils mobiles transforment le paysage des communications et renforcent le besoin de sécurité, car les cyberattaquants exploitent les vulnérabiltés de chaque point d'accès. Le chiffrement de haut niveau, la confidentialité des données et les environnements avec des communications hautement sensibles nécessitent une infrastructure sécurisée, à haute disponibilité, efficace et facile à gérer.

ALE vous recommande d'effectuer les actions suivantes :

Mettez à jour votre système de communication et assurez une surveillance en continu :

- Les mises à jour du système sont d'une importance capitale en termes de cybersécurité. Elles permettent de maintenir votre système de communication à jour et de le protéger contre les vulnérabilités logicielles
- Activez la surveillance de votre système de communication afin de repérer les activités suspectes en configurant des seuils d'utilisation et des alarmes dans le système de gestion du réseau

Mettez en oeuvre l'authentification et le chiffrement :

- Activez l'authentification mutuelle entre tous les appareils (téléphones et passerelles) et le serveur de communication
- Chiffrez la signalisation afin d'éviter les attaques de protocole et les attaques de type « Man-in-the-Middle »
- Chiffrez les communications sur le réseau IP afin d'éviter les écoutes illicites

Optez pour un système de communication redondant et relevez le niveau de sécurité global :

- Le risque zéro n'existe pas. Si une passerelle ou le serveur de communication principal tombe en panne, un serveur de secours va prendre le relais de manière transparente en cas de redondance spatiale
- Ajoutez les composants nécessaires à la protection de votre système de communication, tels qu'un contrôleur de session en bordure (SBC) ou un Reverse Proxy (RP), tandis que les serveurs de notification permettent d'alerter les personnes nécessaires

Sensibilisez les utilisateurs :

- Sensibilisez les utilisateurs et formez les administrateurs ; appliquez les meilleures pratiques au sein de vos équipes, notamment à l'aide de rappels pour la mise à jour des mots de passe, en formant les utilisateurs à la lutte contre la cybercriminalité et en leur apprenant à reconnaître un appel chiffré grâce à l'icône de cadenas sur le téléphone

Pour plus d'informations, consultez nos ressources supplémentaires :

Brochure OmniPCX Enterprise Purple

Fiche technique OmniPCX Enterprise Purple

Livre Blanc - Sécuriser les solutions de communications unifiées et de collaboration

© 2024 ALE International, ALE USA Inc. Tous droits réservés pour tous pays. Le nom et le logo d'Alcatel-Lucent sont des marques commerciales de Nokia utilisées sous licence par ALE. Pour voir la liste des marques de commerce d'ALE, veuillez consulter : www.al-enterprise.com/fr-fr/documentation-juridique/marques-copyright. DID22051201FR (avril 2024)

Alcatel·Lucent Enterprise