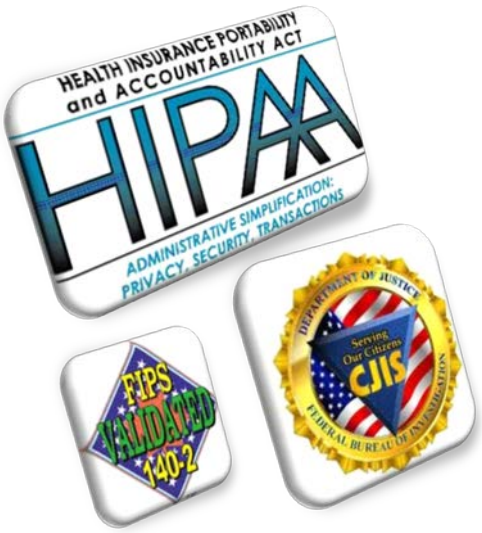
L'accroissement de la main-d'œuvre mobile dans les environnements utilisant des données critiques, comme ceux de la sécurité publique, des soins à domicile et des hôpitaux, pose un défi aux administrateurs de TI. Ils doivent faire en sorte d'offrir des communications sans fil rapides, fiables et transparentes sans toutefois compromettre les mesures de sécurité.

Tous les premiers répondants, qu'ils travaillent dans le domaine municipal, provincial ou fédéral, ont besoin d'un accès rapide et sécuritaire à des renseignements hautement confidentiels, tels qu'antécédents criminels et dossiers médicaux. Le caractère délicat de ces renseignements exige des politiques de sécurité protégeant les données peu importe d'où et comment on les accède.

Sécurité de pointe pour VPN mobile

Conçu tout spécialement pour les organismes transmettant des données critiques et confidentielles sur des connexions VPN mobile, Mult-IP offre persistance et transparence ainsi que sécurité au niveau des utilisateurs, et ce, même lorsque la transmission passe d'un type de réseau à un autre. Mult-IP est compatible avec les plus sévères normes de chiffrement tout en demeurant assez flexible pour que les organismes puissent adapter leurs programmes de sécurité en fonction de leurs besoins, de leurs budgets et de leurs ressources.



Avantages

- Protège l'intégrité des données sans fil transmises
- Valide les appareils clients ainsi que les utilisateurs accédant le réseau
- Simplifie les processus d'authentification sans créer de failles dans la sécurité
- Fait le suivi et enregistre tous les événements de sécurité sur un serveur central

Entrust® Ready

RSA SECURED®

Mobilité sécuritaire

Mult-IP est une solution de VPN mobile qui permet aux mains-d'œuvre mobiles d'accéder aux serveurs d'applications ainsi qu'à d'autres ressources avec un niveau de sécurité se mesurant à celui du LAN de l'entreprise.

Authentification

Mult-IP s'adapte aux environnements d'authentification Windows, RADIUS, Entrust, RSA ou 802.1x (connexion unique), offrant ainsi la protection d'une validation complète sans contraindre les administrateurs à redéfinir les droits d'accès pour chacun des utilisateurs. De plus, si l'appareil client tombe hors couverture, l'utilisateur demeure authentifié pour une période de temps paramétrable, se soldant donc par une persistance de session.

Authentification pour organismes multiples

Un même et unique système Mult-IP permet aux administrateurs de TI de différents organismes de créer leurs propres groupes de clients ayant chacun des procédures d'authentification adaptées à leur budget et leurs besoins spécifiques. Les administrateurs peuvent être liés à un ou plusieurs groupes. À l'aide de droits d'accès, ils peuvent gérer les données étant associées à ces groupes. Cette répartition intelligente des ressources permet à chacun des organismes de définir quel réseau transmettra quelles données selon la priorité, les paramètres d'exploitation ou les exigences concernant la sécurité, et ce, de façon précise pour chacun des groupes de l'organisme ou parmi les autres organismes.

Microsoft® Windows	RADIUS	Entrust®/RSA®	802.1x
fait en sorte que la machine locale demande à l'utilisateur d'entrer son identifiant et son mot de passe lors de la connexion. connexion sur un domaine Windows ; compare les justificatifs d'identité, accessibles à la passerelle Mult-IP par l'entremise du LAN de l'entreprise, avec ceux du *Active Directory*.	utilise le service d'accès au réseau (SAR) pour comparer les justificatifs d'identité de l'utilisateur à ceux d'une base de données centrale. offre des fonctions d'authentification, d'autorisation et de gestion est compatible avec différents protocoles d'authentification, dont point d'accès élargi, EAP, PEAP, CHAP et PAP.	authentification à deux facteurs par matériel ou jeton logiciel avec la passerelle Entrust Identity Guard ou le *RSA Authentication Manager* (aussi connu sous le nom de *RSA appliance*) interfaces serveur RADIUS intégrées, avec les passerelles agissant comme des appareils client	authentification d'appareil client basé sur le port à l'aide du protocole de point d'accès élargi (EAP) mécanisme d'authentification à trois niveaux se composant du client (le suppliant), du contrôleur d'accès (responsable de l'authentification) et du serveur d'authentification Mult-IP agit comme un point d'accès qui ouvre et ferme les canaux de communication de manière indépendante pour chacun des ports virtuels (connexion client) Ouverture de connexion unique ; avec une seule entrée de ses justificatifs d'identité, l'utilisateur obtient accès à une multitude de systèmes sans avoir à les entrer de nouveau

Chiffrement

Mult-IP est un logiciel de VPN mobile certifié conforme à FIPS 140-2 qui offre un chiffrement sur l'ensemble du système en utilisant les algorithmes cryptographiques DES simple, 3DES ou AES (128,192,256). Le logiciel utilise des modules de chiffrement intégrés ayant été certifiés par la *National Institute of Standards and Technology of the United States of America* et le Centre de la sécurité des télécommunications Canada. Mult-IP garantit la sécurité de la connexion dès le départ en utilisant un protocole d'établissement de liaison entre la passerelle et l'appareil client. Les parties se mettent ainsi d'accord sur les règles à utiliser pour les transmissions à venir. Le chiffrement est un réglage de système ne pouvant être restreint à un groupe particulier. La méthode (ou le niveau) de chiffrement la mieux adaptée à un environnement dépend de la solidité et de l'accessibilité des applications et peut être sujette à des restrictions d'exportation à l'extérieur des États-Unis et du Canada.

Version du système d'exploitation	Certificat FIPS 140-2
Windows XP SP3	989
Windows 7	1330
Windows 8.1	1894
Windows Server 2008 R2	1337
Windows Server 2012 R2	1894

Radio IP
Redefining Secure Mobility

Conformité avec la politique gouvernementale

Mult-IP respecte toutes les règles décrites dans la version 5.2 de la politique de sécurité du U.S. *Department of Justice – FBI Criminal Justice Information Services (CJIS)* ainsi que dans les versions les plus récentes du *Health Insurance Portability and Accountability Act (HIPAA)* et du *Health Information Technology for Economic and Clinical Health Act (HITECH)*. Mult-IP dépasse les exigences du FBI CJIS du HIPAA et du HITECH en offrant les chiffrements FIPS 140-2, AES (128, 192, 256) et 3DES de même que l'authentification à deux facteurs.

FBI CJIS

Mult-IP observe les sections applicables de la version 5.2 de la politique du CJIS. La politique fournit les contrôles nécessaires pour protéger l'ensemble du cycle de vie des renseignements *Criminal Justice Information (CJI)*, qu'ils soient enregistrés ou en transit.

Chiffrement (Section 5.10.1.2)	**Identité de l'utilisateur (Section 5.6.1)**	**Authentification avancée (Section 5.6.2.2)**
« Lorsque des renseignements CJIS sont transmis à l'extérieur des limites physiques de l'emplacement sécurisé, les données doivent être immédiatement protégées à l'aide de mécanismes cryptographiques (chiffrement) ».	*« Toute personne autorisée à (...) transmettre des renseignements CJI doit posséder une identité unique. Une identité unique est aussi requise pour toutes les personnes qui gèrent ou entretiennent le ou les systèmes accédant à des renseignements CJI ou des réseaux par où transitent de tels renseignements ».*	*« Une authentification avancée amène une sécurité additionnelle à la confirmation habituelle de l'identité de l'utilisateur et à l'authentification de l'adresse IP et du mot de passe ».*
→ Mult-IP respecte l'utilisation obligatoire du chiffrement certifié FIPS 140-2 au niveau minimum de 128 bits. → La clé symétrique est chiffrée par un algorithme cryptographique RSA de 2048 bits certifié FIPS 140-2 comme recommandé par le *NIST* (*National Institute of Standards and Technology*, *Special Publication* 800-56B et 800-131A).	→ Mult-IP est compatible avec les méthodes d'authentification des appareils client suivantes : authentification Windows, RADIUS, 802.1x et Entrust/RSA.	→ Mult-IP offre aussi l'authentification à deux facteurs pour confirmer l'identité de l'utilisateur. L'authentification à deux facteurs est un protocole de sécurité par lequel l'identité d'un utilisateur est confirmée à l'aide de deux (2) sources utilisant les méthodes approuvées suivantes : • un jeton ou une clé automatiquement générée par un logiciel ou un appareil • un mot de passe ou un code de sécurité défini et entré par l'utilisateur • une lecture biométrique (c'est-à-dire, une empreinte digitale, une lecture de l'iris, etc.) → Mult-IP donne la possibilité de combiner ces méthodes : RADIUS, cartes à puce, ICP (infrastructure à clés publiques), biométrie.

HIPAA et HITECH

HIPAA et HITECH définissent les règles de confidentialité et de sécurité protégeant les dossiers médicaux — *Electronic Protected Health Information* (*EPHI*).

Contrôle d'accès	Contrôles de vérification	Intégrité	Authentification de personne ou d'entité	Sécurité des transmissions
§ 164.312(a)(1) : *« la capacité ou les moyens nécessaires pour lire, écrire, modifier ou communiquer des données ou des renseignements, ou autrement utiliser n'importe quelle ressource du système. »* **§ 164.312(a)(2)(i) :** *« Assigner un nom ou un numéro unique qui servira à déterminer l'identité des utilisateurs et à faire leur suivi de ceux-ci. »* **§ 164.312(a)(2)(iii) :** *« Mettre en place des procédures électroniques qui terminent une session électronique après une période de temps d'inactivité prédéterminée. »* **§ 164.312(a)(2)(iv) :** *« Mettre en place un mécanisme pour chiffrer et déchiffrer les dossiers médicaux électroniques. »*	**§ 164.312(b) :** *« Mettre en place des mécanismes matériels, logiciels ou procéduraux qui enregistrent et étudient l'activité dans les systèmes d'information contenant ou utilisant des dossiers médicaux électroniques. »*	**§ 164.312(c)(1) :** *« la confirmation que les données ou les renseignements n'ont pas été modifiés ou détruits sans autorisation. »* *« Mettre en place des politiques et des procédures protégeant les dossiers médicaux électroniques de toutes modifications ou destructions non autorisées. »* **§ 164.312(c)(2) :** *« Mettre en place des mécanismes électroniques pouvant confirmer que les dossiers médicaux électroniques n'ont pas été modifiés ou détruits sans autorisation. »*	**§ 164.312(d) :** *« Mettre en place des procédures pour garantir qu'une personne ou une entité tentant d'accéder des dossiers médicaux électroniques est bien qui elle prétend être. »*	**§ 164.312(e)(1) :** *« Mettre en place des mesures techniques de sécurité pour prévenir tout accès non autorisé aux dossiers médicaux électroniques lors de leur transmission sur des réseaux de communications électroniques. »* **§ 164.312(e)(2)(i) :** *« Mettre en place des mesures de sécurité garantissant que les dossiers médicaux électroniques transmis ne sont pas modifiés sans détection jusqu'à ce qu'on décide qu'ils ne sont plus utiles. »* **§ 164.312(e)(2)(ii) :** *« Mettre en place un mécanisme pour chiffrer les dossiers médicaux électroniques lorsque jugé approprié. »*
• Les clients Mult-IP et les administrateurs ont une identité distincte et sont authentifiés de manière unique. • Persistance de session : garantit que les appareils client se reconnectant après une certaine période de temps prédéterminée sont forcés de se réenregistrer. • Mult-IP est compatible avec les algorithmes cryptographiques DES unique, 3DES, et AES (128,192,256) utilisant FIPS 140-2.	• Le journal d'exploitation de Mult-IP fait le suivi des événements relatifs aux activités, aux changements de statut et de conditions générales diverses sur les appareils mobiles client. • Le module analytique de Mult-IP vient avec 25 modèles de rapport en format Excel® dessinant un portrait détaillé du réseau et de l'utilisation des applications.	• Mult-IP garantit l'intégrité des données et protège contre les modifications et les destructions non autorisées à l'aide de l'authentification et du chiffrement. • Les protocoles de tunnellisation cryptographique de Mult-IP, en tant que VPN mobile, certifient la confidentialité en bloquant les interceptions et le reniflage de paquets et en permettant à l'authentification de l'expéditeur de bloquer la mystification d'identité. Ils fournissent aussi un message intègre en prévenant toute modification à celui-ci.	• Mult-IP offre une authentification à deux facteurs sécuritaire (mot de passe, jeton, biométrie, etc.) pour prouver l'identité lors de l'authentification.	• Mult-IP chiffre toutes les données pour protéger l'intégrité des dossiers médicaux électroniques et empêcher tout accès non autorisé lors de la communication sur les réseaux. • Les protocoles de tunnellisation cryptographique de Mult-IP, en tant que VPN mobile, certifient la confidentialité en bloquant les interceptions et le renfilage de paquets et en permettant à l'authentification de l'expéditeur de bloquer la mystification d'identité. Ils fournissent aussi un message intègre en prévenant toute modification à celui-ci. • Mult-IP utilise des algorithmes cryptographiques 3DES et AES certifiés FIPS 140-2.