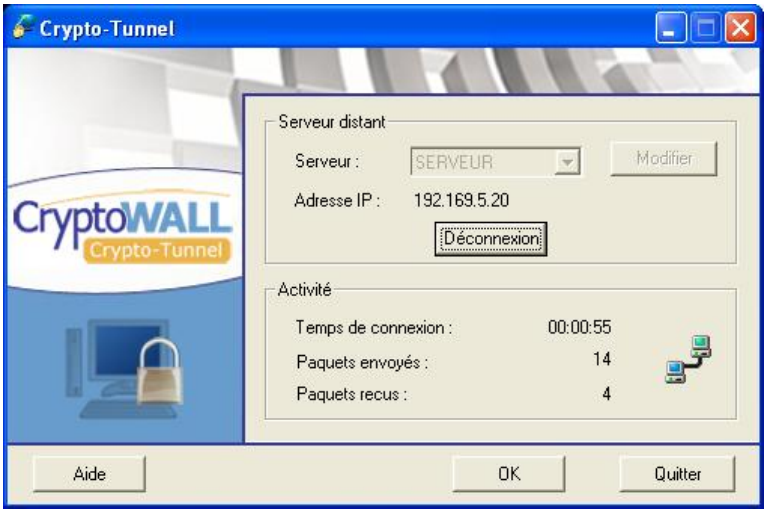
amesys

CryptoWALL Crypto-Tunnel

CRYPTOWALL CRYPTO-TUNNEL CLIENTS-SERVEUR

UN TUNNEL SECURISE POUR ETENDRE VOTRE RESEAU LOCAL



CONNECTEZ VOS POSTES NOMADES A VOTRE SERVEUR EN TOUTE SECURITE

CryptoWALL Crypto-Tunnel Clients-Serveur établit des tunnels sécurisés entre un serveur, généralement placé sur le site central de votre établissement, et les postes clients nomades qui ont besoin d'être reliés au réseau local de l'entreprise. Cette solution logicielle a été conçue pour permettre à vos collaborateurs d'accéder en toute sécurité au réseau de l'entreprise où qu'ils se trouvent dans le monde. Chacun pourra échanger en toute confidentialité tous types d'informations

PRINCIPALES CARACTERISTIQUES

- VPN client windows / VPN serveur linux
- Authentification des extrémités par ECC
  (courbes elliptiques sur support matériel Token USB)
- Chiffrement des communications IP en AES ou propriétaire
- Gestion automatique des clés de chiffrement
- Détection des tentatives d'intrusion et blocage de toutes les communications non chiffrées

AES
Advanced Encryption Standard

ENVIRONNEMENT

Le système de « Tunnel » sécurise les communications entre le réseau local et les postes clients où qu'ils se trouvent. Les données circulent chiffrées sur le réseau et ne pourront être accessibles ni par un pirate ni par un intrus. Le lien chiffré est établi entre le site distant et les postes nomades quel que soit le media physique utilisé : Ethernet, WiFi, fibre optique, Bluetooth, IRDA, ….

UNE SOLUTION QUI AGIT COMME UN FIREWALL POUR PREVENIR TOUTES SORTES D'INTRUSIONS

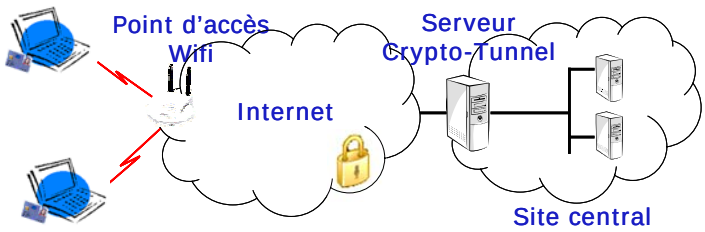
Le logiciel sur le poste client est intégré au système Windows au niveau du driver, ce qui lui permet de contrôler et de sécuriser tous les flux réseaux entrants et sortants. Ainsi, pendant la communication sécurisée, tous les ports réseau sont fermés hormis le port chiffré. Le logiciel installé sur le serveur intègre toujours une technique de détection d'intrusion. Cette technologie rend votre serveur beaucoup plus sûr et insensible aux différentes attaques qu'il pourrait subir : Man in the middle, attaque par rebond, Spoofing, Flooding, etc.

SIMPLE A DEPLOYER ET A UTILISER

Quelque soit l'algorithme de chiffrement choisi par l'utilisateur, Crypto-Tunnel Point à Point intègre toujours une technique de détection d'intrusion. Cette technologie rend votre serveur beaucoup plus sûr et insensibles aux différentes attaques qu'il pourrait subir : Man in the middle, Attaque par rebond, Spoofing, Flooding, etc.

RESPECT DES NORMES ET STANDARDS EUROPEENS ET INTERNATIONAUX

L'installation de ce système ne demande aucune configuration spécifique et est transparente pour l'utilisateur. Chaque utilisateur conserve son confort de travail habituel, Crypto-Tunnel Clients-Serveur permet d'utiliser de manière sécurisée toutes les applications courantes : Mail, Internet, Communication audio, Vidéo conférence ou n'importe qu'elle application métier spécifique. Le système sécurise vos échanges d'informations sensibles quel qu'en soit le type.



UNE AUTHENTIFICATION FORTE PAR SIGNATURE ECC COUPLE A UN CHIFFREMENT STANDARD OU PROPRIETAIRE

Avec un protocole d'échange de clés basé sur la technologie des courbes elliptiques, Crypto-Tunnel Clients-Serveur renforce encore plus le processus d'authentification. Le système de chiffrement utilisé est quant à lui laissé au choix du client : l'utilisation de l'algorithme standard AES avec une sécurité de 128 ou 256 bits ou l'utilisation de algorithme de chiffrement propriétaire de CryptoWALL.

RESPECT DES NORMES ET STANDARDS EUROPEENS ET INTERNATIONAUX

CryptoWALL Crypto-Tunnel Clients-Serveur est conforme aux normes et standards européens et internationaux, relatifs à la sécurité des systèmes d'information qui garantissent la compatibilité et l'évolutivité de ses solutions : implémentation des algorithmes de chiffrement AES, certificats numériques au format X509 V3 pour l'authentification, signature en courbes elliptiques ECC/DSA…

DETAILS TECHNIQUES

Serveur sécurisé Linux Client Windows 2000, XP Plate-forme logicielle Authentification X509V3 & ECC (courbes elliptiques) Authentification par clé USB à puce	Algorithmes de chiffrement AES ou propriétaire Clés de chiffrement 128 à 256 bits ou spécifique Blocage des clés en mémoire vive Compatible Wi-Fi, Ethernet, Radio Authentification mutuelle des extrémités Sécurité administrateur, supervision du trafic & logs

LES SPECIFICATIONS MENTIONNEES CI-DESSUS SONT SUSCEPTIBLES D'ETRE MODIFIEES SANS PREAVIS.

HEADQUARTERS
1030 Av. Guillibert de la Lauzière- Les Milles
BP 20 140 - 13794 AIX EN PROVENCE Cedex 3
Tel. +33 (0)4 42 60 70 00 - Fax. + 33 (0)4 42 60 00 26
contact-us@amesys.fr