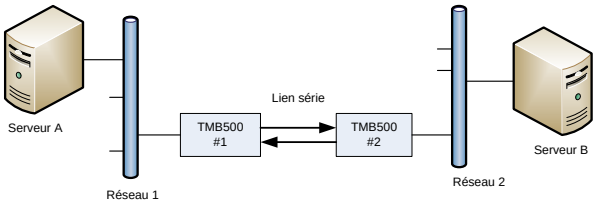
Ligne de produits sécurisés TMB500

Passerelle avec rupture de protocole

Le TMB500 permet de réaliser une passerelle entre deux réseaux avec une rupture de protocole garantissant l'étanchéité entre les deux réseaux.
Il répond particulièrement bien aux problématiques de sécurité informatique pour notamment le transfert d'informations de temps (trames de temps numériques ou NTP).

Le schéma ci-dessous présente le principe de la passerelle en utilisant deux équipements TMB500.



Les deux équipements peuvent être distants jusqu'à 1km sans ajout d'extendeur.

Les plages d'adressage des deux réseaux sont complètement séparées, chaque serveur n'a à connaître que l'adresse et le port de la passerelle. Chaque équipement TMB500 n'a à connaitre que les caractéristiques du réseau auquel il est connecté.

Lien série

Le lien série reliant les deux passerelles est soit un lien RS422, soit un lien optique sur fibre optique multi-mode.

Le lien est bidirectionnel pour supporter des protocoles tels que NTP mais il est possible de faire fonctionner la passerelle avec un lien unidirectionnel et ainsi la transformer en diode réseau.

Pile TCP/IP

La pile TCP/IP utilisée dans l'équipement a été développée par Timelink et a été adaptée particulièrement aux fonctions requises pour plus de sécurité.

L'équipement gère les protocoles ARP, ICMP et UDP.

Pare-feu

L'équipement intègre un pare-feu qui filtre le trafic entrant :

- Rejet des protocoles non autorisés
- Vérification de l'adresse IP de la source par rapport à une liste blanche (ICMP requête ping et UDP)
- Vérification du port destinataire
- Vérification optionnelle du port source
- Détection du changement d'adresse MAC sur les communications établies

Configuration

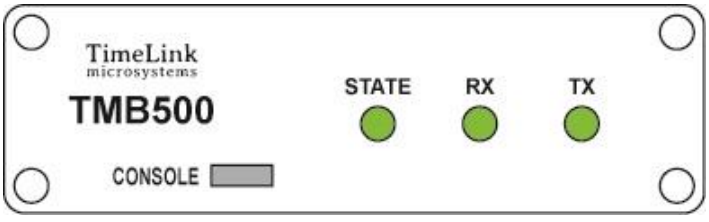
La configuration est stockée dans l'équipement dans une mémoire Flash. Elle est modifiable depuis la liaison console via un menu simple. L'accès à la console est protégé par mot de passe.

Surveillance et statistiques

L'équipement mémorise dans une mémoire circulaire les adresses IP et les ports des trames qui ont été rejetées afin de détecter la source d'attaques éventuelles ou simplement des erreurs de configuration. Cette mémoire est consultable par la liaison console.

Principe de fonctionnement

La passerelle utilise uniquement le protocole UDP. A chaque port de destination autorisé correspond un canal de communication qui va transmettre le contenu de la charge utile du datagramme UDP via le lien série. Le contenu de la charge utile du datagramme UDP est transmis tel que et peut donc être chiffré ou non. A la réception de la trame série, le contenu utile est émis vers le destinataire défini dans la configuration.



Face avant

Caractéristiques

Ethernet

Interface 10/100 Mbs
Connecteur RJ45

Protocoles ARP, ICMP (ping), UDP

Pare-feu : filtrage adresse IP, port destinataire, port source optionnel, adresse MAC sur communication en cours

Liaisons Séries

Vitesse maximale 115200 bauds

1 liaison série asynchrone avec interface électrique RS422
Connecteur SubD 9 points

1 liaison optique bidirectionnelle pour fibre multi-mode
Connecteurs SC

Bande passante

La bande passante est limitée par le débit de la liaison série. La bande passante en nombre de trame par seconde (pour une direction donnée) est obtenue par la formule :

10000 / <nombre d'octets de la charge utile>

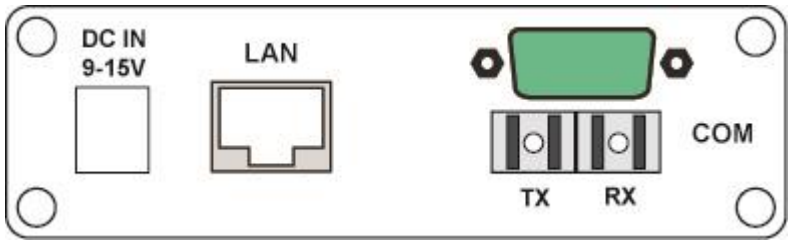
Par exemple pour NTP, le nombre maximum de requêtes/réponses par seconde est d'environ 100.

Console

Configuration et surveillance par liaison série sur interface USB.
Connecteur USB type mini B.

Energie

Alimentation boîtier : 9-18V DC
Consommation : AD
Connecteur jack
Alimentation secteur par boîtier externe fourni.



Face arrière