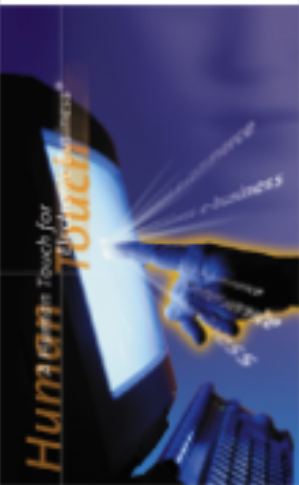


# Protéger le réseau d'entreprise

M > Wall™

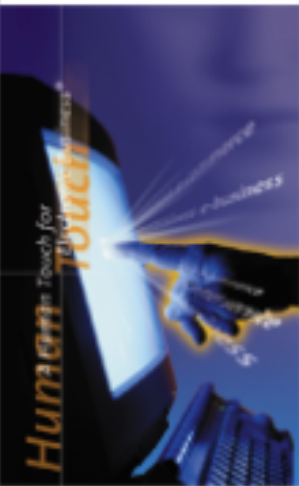


*Présentation OSSIR  
8 octobre 2001*

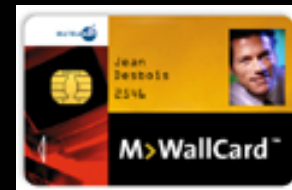
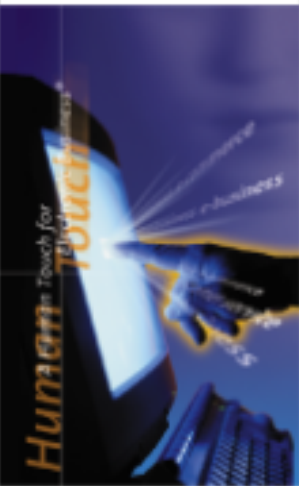


- **MATRAnet : Editeur de logiciels de Sécurité**
- **Créée en 1996 ; 55 employés**
- **Réseau international de partenaires**
- **Siège à Vélizy, bureaux en Asie et Espagne**

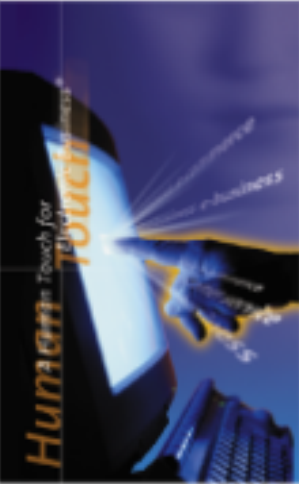
MATRAnet, membre **d'EADS Telecom**, propose une suite de solutions logicielles intégrées, le **MATRAnet Security Framework**, garantissant la sécurité de bout en bout des applications Internet de l'Entreprise grâce à une architecture commune.



- Pour conduire **en toute sécurité** des affaires ou des relations sur l'Internet avec leurs clients, leurs fournisseurs et leurs partenaires, les sociétés ont besoin :
  - **de protéger** leurs informations et données confidentielles contre des sources non autorisées.
  - **de garantir** l'intégrité et la confidentialité de toute information échangée.
  - **d'authentifier** les utilisateurs et les applications.
  - **de gérer** et contrôler la navigation des employés.
  - **de détecter** les intrusions et les attaques potentielles pour réagir de manière appropriée.
- Pour garantir **une sécurité efficace de bout en bout**, les sociétés ont besoin de solutions intégrées qui leur permettent de définir et de gérer une politique de sécurité.



## Le MATRAnet Security Framework



- **pour protéger** et donner accès aux informations et données confidentielles.

**Firewall applicatif : M>Wall**

- **pour garantir** l'intégrité et la confidentialité de toute information échangée.

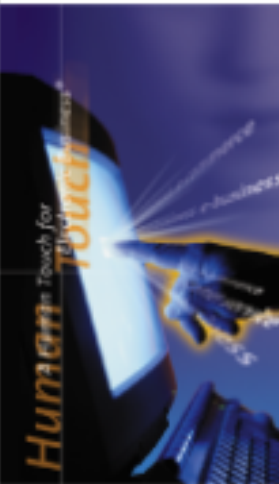
**Réseau Privé Virtuel : M>Tunnel**

- **pour authentifier** les utilisateurs et les applications.

**Authentification forte par carte à puce : M>WallCard**

- **pour améliorer** le contrôle de l'information.

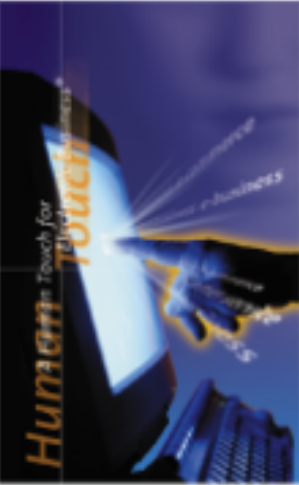
**Administration des accès Web : M>Manager**



# M > Wall™

MATRAnet Confidentiel

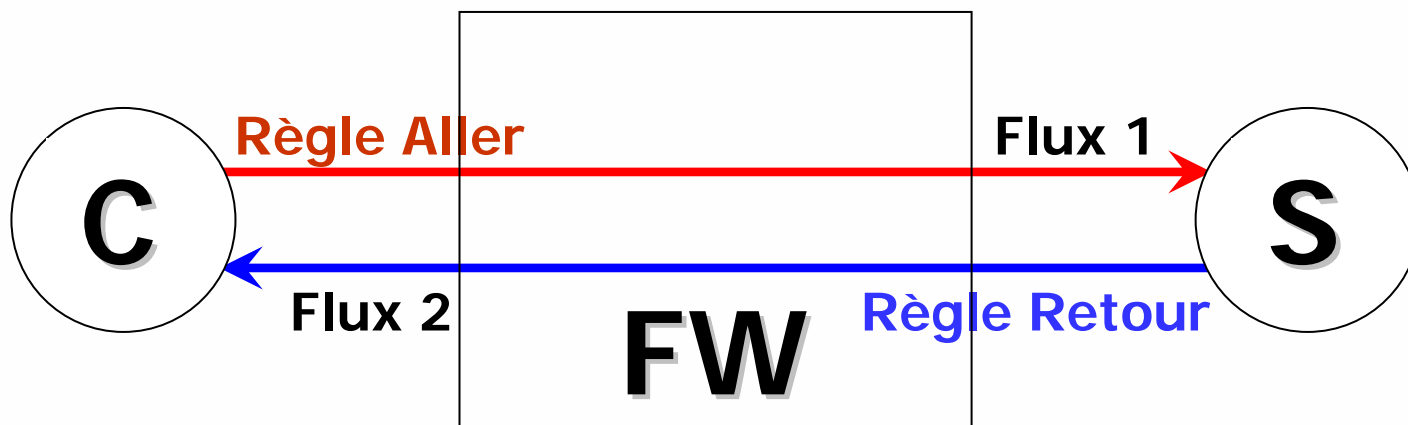
Le coupe-feu applicatif



1. Filtre de paquets statique
2. Filtre de paquets dynamique
3. Filtrage applicatif
4. Adaptive Proxy

- **Choix du niveau de sécurité pour chaque flux et donc chaque application**

- Contrôle des paquets au niveau réseau.
- Avantages : rapidité
- Inconvénient : pas de contrôle des données.



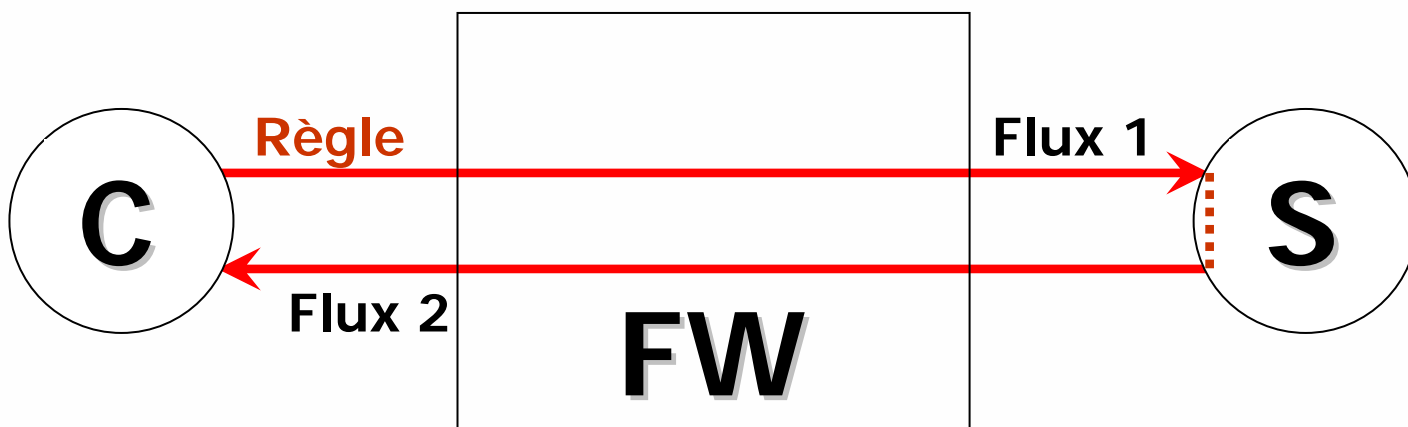
2 règles

**C** = client

**FW** = firewall

**S** = serveur

- Sécurité au niveau des connexions réseau.
  - Une seule règle : le flux retour est géré dynamiquement.
- ➔ La connexion n'est possible que dans un sens
- Avantages : rapidité, sécurité accrue



1 seule règle

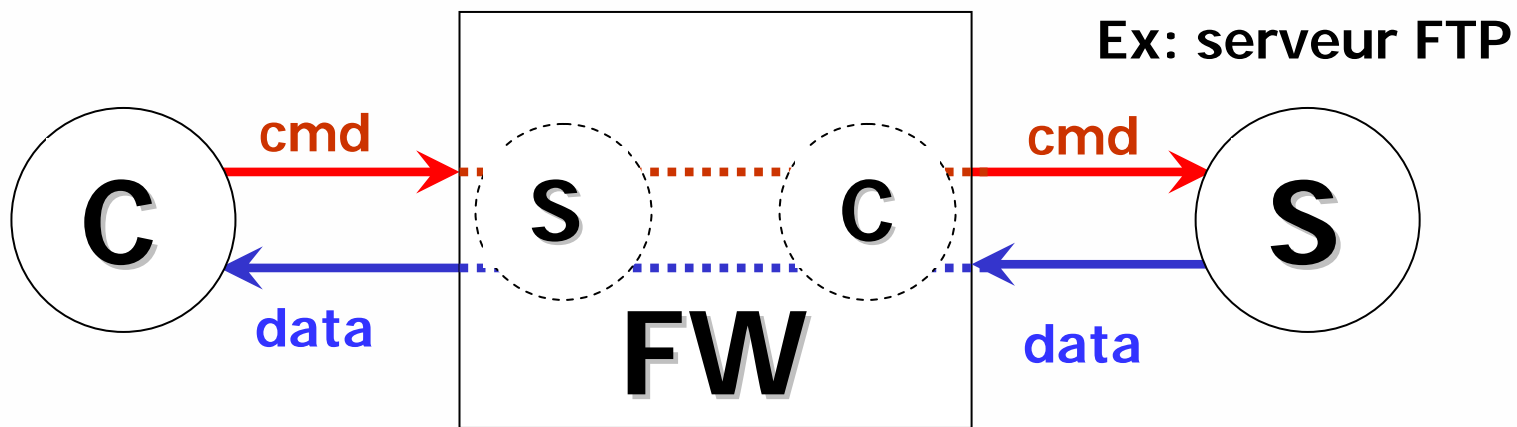
**C** = client

**FW** = firewall

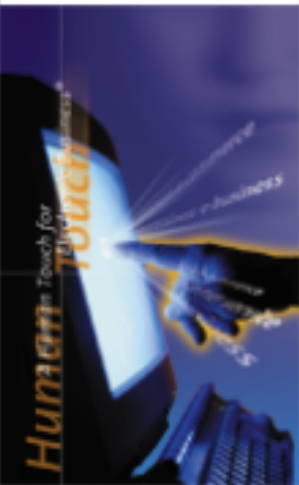
**S** = serveur

- Filtre au niveau des applications et des données grâce aux proxies.

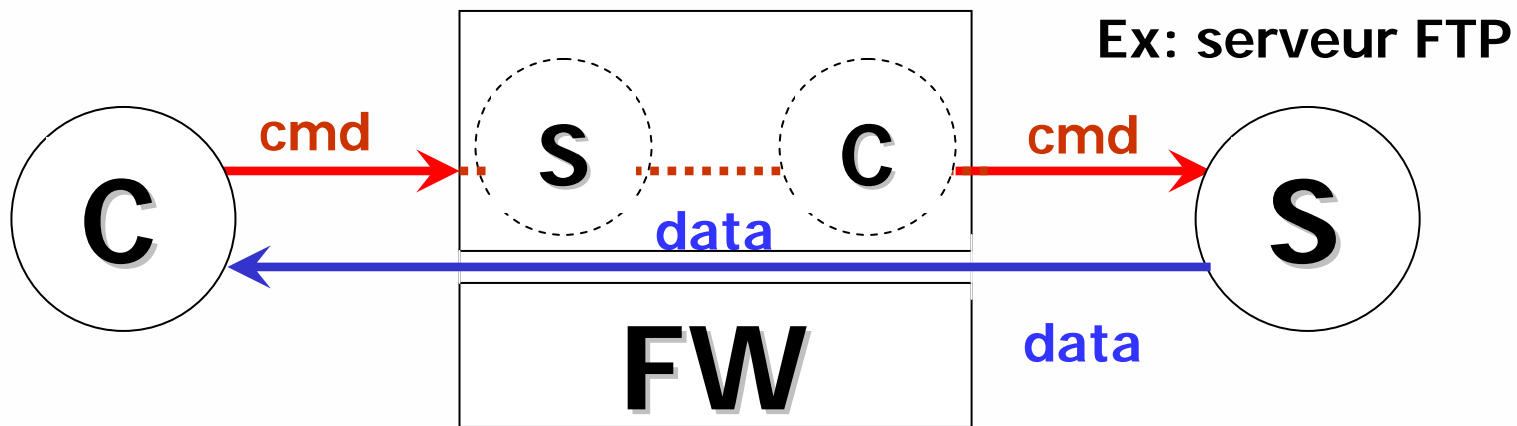
Avantages : **La vraie sécurité au niveau des données applicatives**



(C) = client      (S) = serveur fictif      (C) = client fictif      (S) = serveur  
 cmd = commande      FW = firewall      data = données



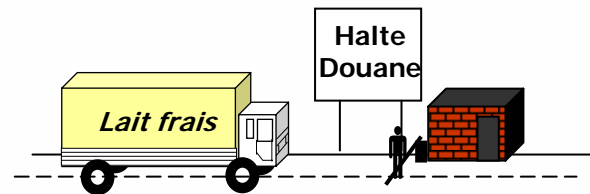
- Le flux de données n'est pas traité, seules les commandes sont analysées.
- Avantages : Sécurité et vitesse optimisées.



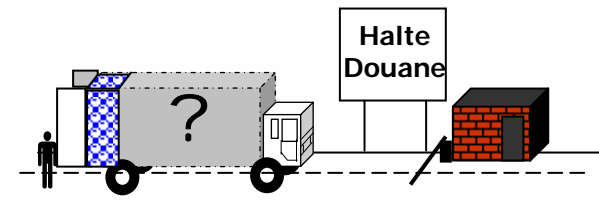
adaptative proxy

(C) = client      (S) = serveur fictif      (C) = client fictif      (S) = serveur  
 cmd = commande      FW = firewall      data = données

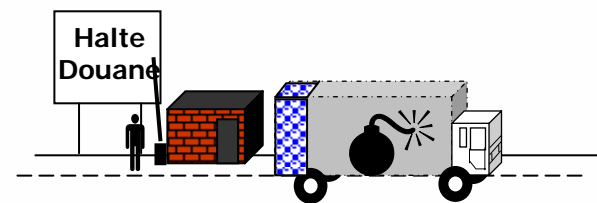
## Méthode Statefull Inspection (filtre de paquet + tables d'état)



Un camion arrive à une frontière

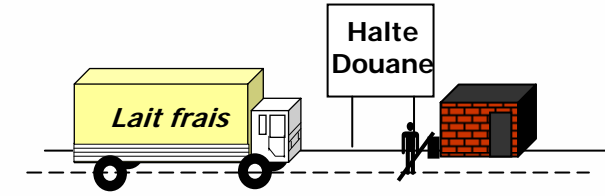


Le douanier inspecte la première couche de la cargaison

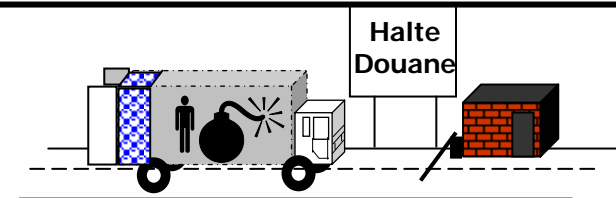


Le douanier n'a vu que du lait. Le lait étant autorisé dans ses tables d'état, il laisse passer le camion...

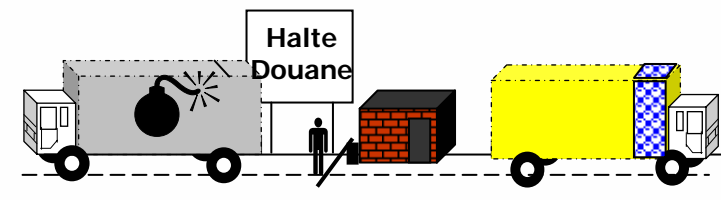
## Méthode d'inspection Haute sécurité M>Wall (filtre applicatif/proxies)



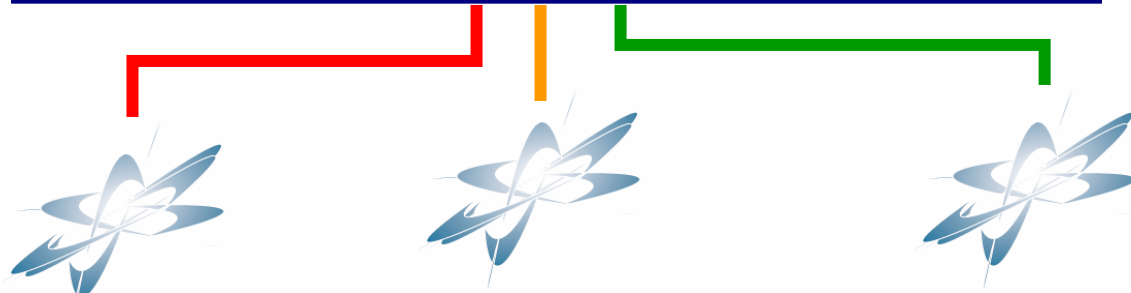
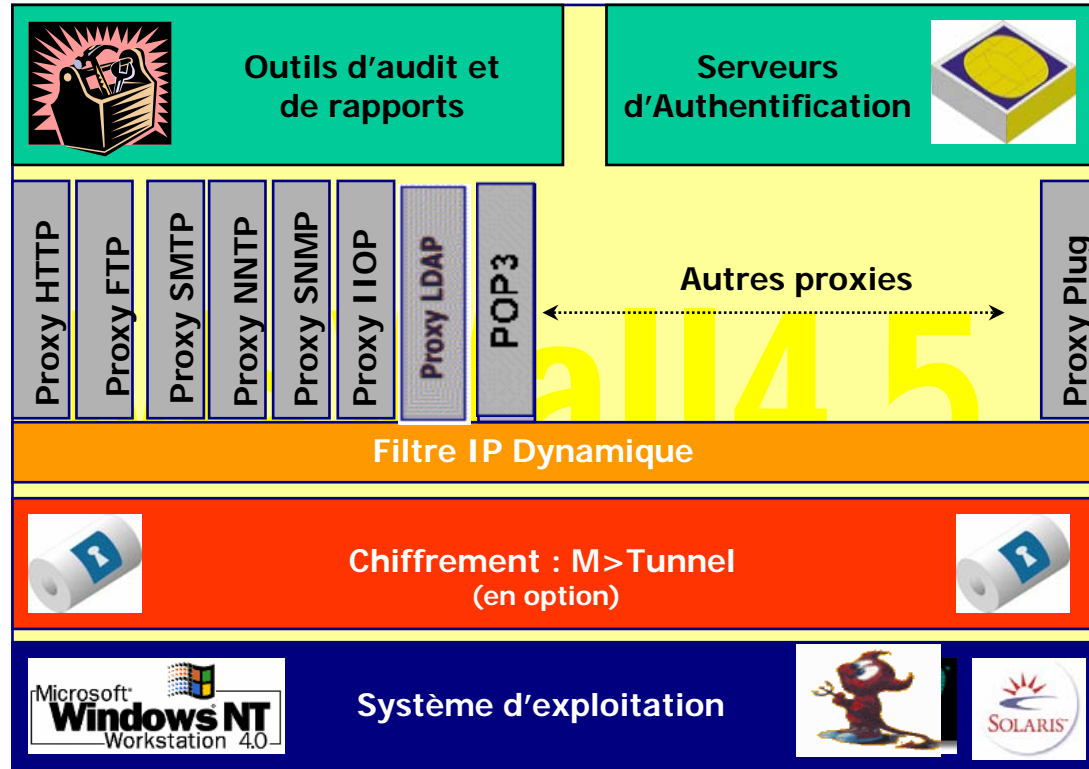
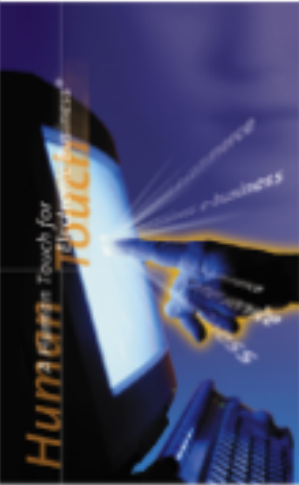
Un camion arrive à une frontière



Le douanier inspecte toute la cargaison en détail



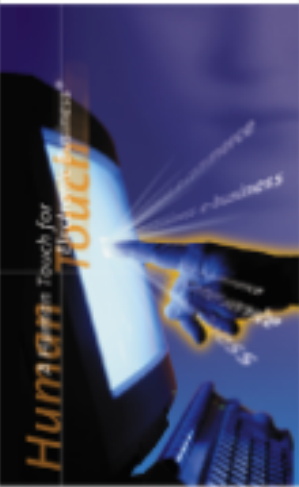
Le douanier transfère la cargaison autorisée dans un nouveau camion, la cargaison dangereuse est refoulée.



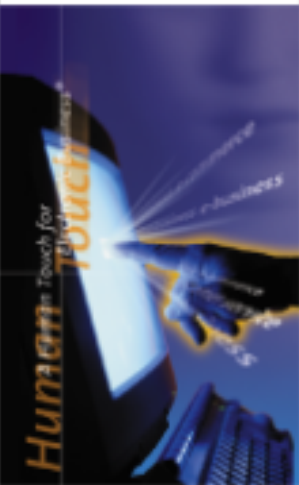
Interface Externe

Interfaces DMZ

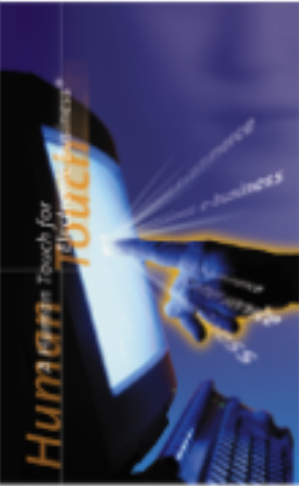
Interface Interne



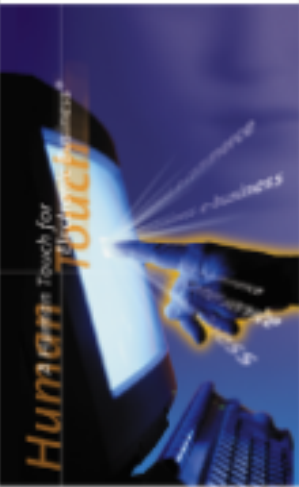
- **Filtre de paquets statique :**  
Protocole, interface, flag de protocole, adresses et ports sources, adresses et ports destinations, règle spécifique pour paquet sortant de M>Tunnel.
- **Filtre de paquets dynamique :**  
Idem + Masquage d 'adresse.
- **Translation d'adresses statique ou dynamique.**



- **Web:** HTTP
- **Messagerie électronique:** SMTP, POP3
- **Transfert de fichiers:** FTP
- **Connexion en mode terminal:** TELNET, rlogin, rsh
- **News:** NNTP
- **Impression:** LP
- **X-Window:** X11
- **Multimédia:**  
Real Audio, Real Video, Netshow, VDOLive, H323
- **Administration réseau:** SNMP
- **Accès bases de données:** Sybase, SQLNet, MS SQL
- **e-Business:** IIOP
- **Annuaire:** LDAP
- **GroupeWare/messagerie:** Lotus Notes
- **Proxies génériques:** pour support d'autres services



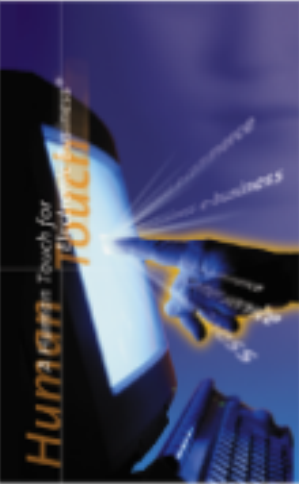
- Cache d'authentification, pour accélération des performances.
- Partage d'authentification entre les Proxy (Single Sign On).
- Partage d'authentification entre M>Wall et M>Tunnel au niveau noyau (au niveau Proxy dans la prochaine version)

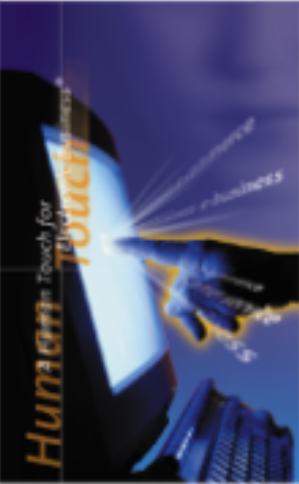


- Bases d 'utilisateurs internes
- Ouverture vers des bases LDAP externes.
- Authentification forte M>WallCard au niveau Proxy.
- Support de systèmes d'authentification tiers de type : RADIUS, SecureID, ActivCard, SNK, S/Key, Defender, Digipass, CRYPTOcard ...



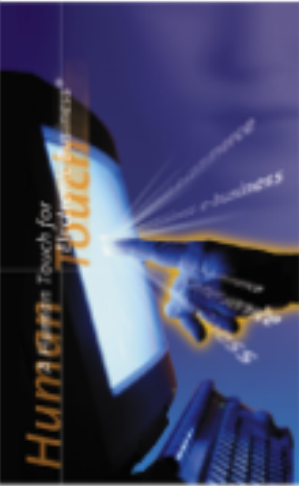
- Interface conviviale, permettant un paramétrage facile et fin pour tous types de configuration, de la plus simple à la plus complexe.
- Administration de tous les produits du MATRAnet Security Framework dans la même interface.



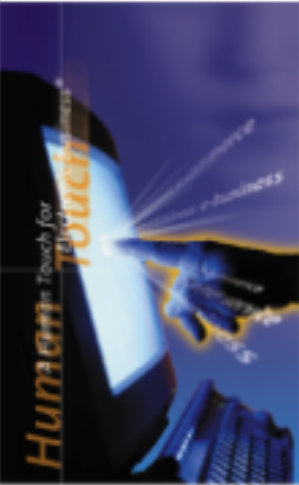


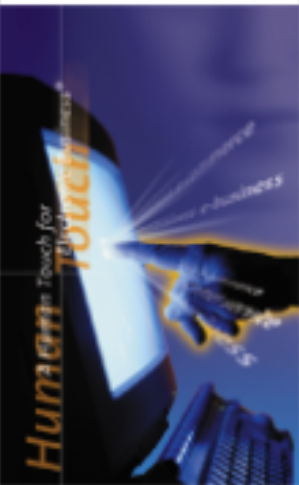
- **Solution à grandes capacités**
- Facilité d'installation
- Adaptabilité au réseau, solution qui s'adapte à des configurations :
  - multiples interfaces réseaux
  - multi-processeurs
- Adaptabilité à l'OS, suit les capacités de traitement de l'OS.

- **BSD/OS** : Unix pour PC reconnu par les experts pour sa sécurité. Licence de l'OS fournie avec M>Wall.
- **Solaris** : OS sûr avec une gamme de machines qui permet une évolution vers de grosses configurations.
- **NT** : OS facile d'abord pour ceux qui ne connaissent pas l'environnement Unix.



- Depuis le 18 mai 2001, M>Wall a reçu par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), la certification ITSEC E3.
- ➔ Plus haut niveau de certification au niveau européen pour des produits non militaires





# Questions ?

Pour plus d'informations :  
<http://www.matranet.com>  
Tel : 01 34 58 44 00