THEGREENBOW FIREWALL DISTRIBUE
TGB::BOB! Pro

Spécifications techniques

SISTECH SA
THEGREENBOW
28 rue de Caumartin
75009 Paris

Tel.: 01.43.12.39.37
Fax.:01.43.12.55.44

E-mail: info@thegreenbow.fr
Web: www.thegreenbow.fr

1 Problématique

Avec l'évolution des modes de communication en entreprise, les types de vulnérabilités augmentent :

- Les postes nomades, utilisés pour se connecter alternativement sur le site de l'entreprise et sur Internet, sont les cibles privilégiées pour l'installation de chevaux de Troie, devenant ainsi autant de passerelles d'accès au réseau d'entreprise.
- Les postes connectés au réseau local de l'entreprise font, quant à eux, l'objet d'attaques perpétrées à l'intérieur même de l'entreprise : destruction de fichiers, espionnage interne, déclenchement de crash à distance, etc…
- Enfin, les postes équipés d'une connexion directe par modem sont des points d'entrée appréciés pour les attaques externes.

Vis à vis de ces nouvelles vulnérabilités, il est strictement nécessaire aujourd'hui d'étendre la protection du réseau d'entreprise à son niveau le plus sensible : le poste lui-même. C'est le rôle d'un firewall personnel.

Cette protection est d'autant plus efficace en entreprise qu'elle est gérée de façon centralisée. C'est le rôle du serveur d'administration du parc de firewalls installés.

2 Solution

TGB::BOB! est un firewall personnel qui sécurise toutes les communications entrantes et sortantes d'un ordinateur. Il protège ainsi le poste contre :

- les attaques venant d'Internet sur le poste du particulier comme sur le poste en entreprise, fixe ou nomade (vol ou destruction de données, blocage de la machine, intrusion)
- les attaques internes à l'entreprise en protégeant le poste vis à vis du réseau interne (espionnage, vol de données, intrusion)
- les utilisations de la station à l'insu de son utilisateur (cheval de Troie, rebond).

Associé à une administration centralisée, le firewall personnel TGB::BOB! représente la solution pour distribuer efficacement la sécurité à tout le réseau d'entreprise.

Cette administration permet l'élaboration et la distribution des règles de sécurité, la supervision des alarmes, la gestion globale du parc installé (création et suppression de comptes utilisateurs).

Pour être parfaitement efficace, une solution de sécurité administrée doit clairement offrir :

1. Une simplicité d'emploi maximale pour les utilisateurs finaux, sous peine de voir la solution inutilisée ou pire, contournée. L'utilisateur doit en effet pouvoir facilement se protéger contre les dénis de service, l'espionnage local, les communications non contrôlées vers Internet (installation de programme, cheval de Troie).
2. Une grande précision des configurations pour l'administrateur. Cette précision doit en effet permettre la définition d'une politique globale de sécurité allant du filtrage des accès vers l'extérieur jusqu'à la mise en œuvre de "garde-fous" contre les erreurs de manipulation.

3 Le firewall distribué : TGB::BOB! Pro

La solution TGB::BOB! Pro se compose du centre d'administration BOB::ADMIN, hébergé sur un serveur, et de l'ensemble des firewalls personnels TGB::BOB installés sur chaque poste à protéger.

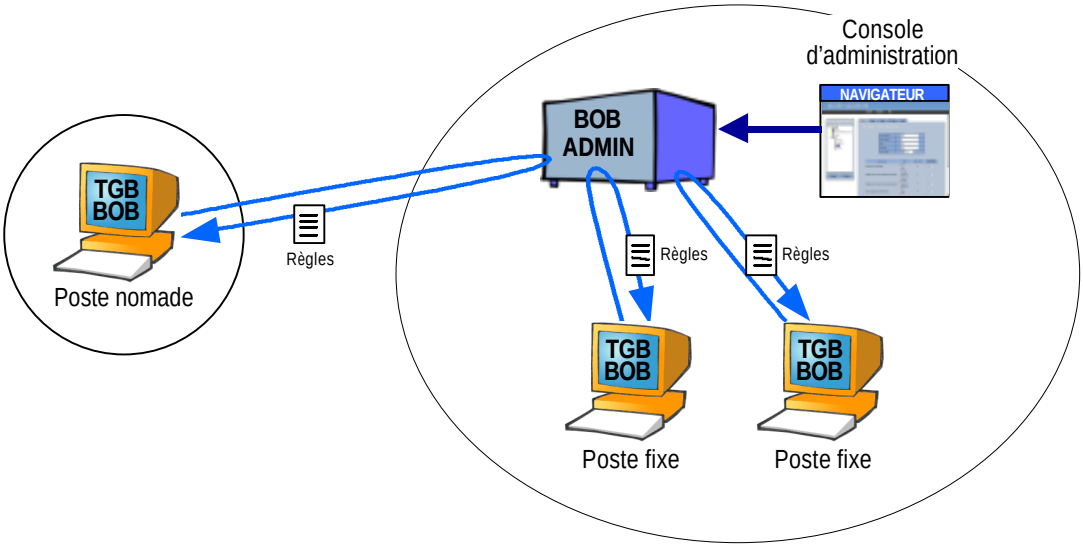


Fig. 1 Solution TGB::BOB! Pro

3.1 Firewall personnel

TGB::BOB! est un firewall personnel pour plates-formes Windows 95, 98, Millenium, NT4, 2000, XP.

Il sécurise toutes les communications entrantes et sortantes du poste à protéger, que ce dernier soit connecté directement au réseau d'entreprise, ou qu'il soit connecté directement à Internet.

Toutes les communications sont soumises à un ensemble de filtres élaborés soit par le firewall lui-même (par exemple pour la protection contre les dénis de service) soit sur décision de l'utilisateur (figure ci-dessous).

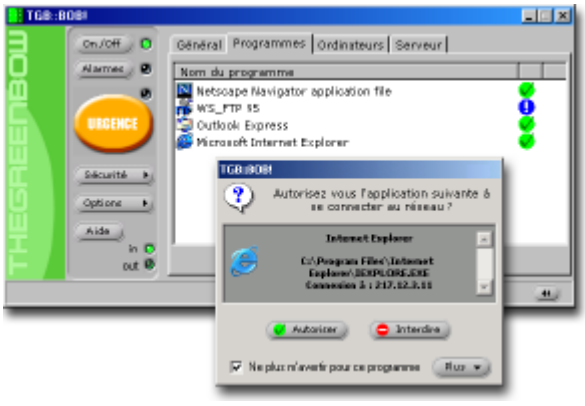


Fig. 2 Interface du firewall personnel

TGB::BOB! implémente une technologie de filtrage à deux niveaux qui garantit le contrôle de toutes les connexions entrantes et de toutes les applications sortantes. Ces dernières sont de plus signées pour protéger le poste contre des chevaux de Troie usurpant l'identité de programmes classiques.

TGB::BOB! protège des attaques typiques en provenance d'Internet (déni de services, exploits, scans d'adresses ou de ports), mais aussi des attaques perpétrées sur le réseau d'entreprise (espionnage ou malveillance via l'utilisation entre autres des ressources Windows tel que le partage de fichiers). TGB::BOB! protège enfin le poste contre les chevaux de Troie en les empêchant de communiquer avec l'extérieur du poste.

L'ergonomie particulièrement étudiée de TGB::BOB! en fait un produit extrêmement simple à utiliser, depuis son installation jusqu'à sa configuration. Toute la puissance technique du firewall est masquée pour n'offrir à l'utilisateur qu'un nombre restreint de sollicitations simples.

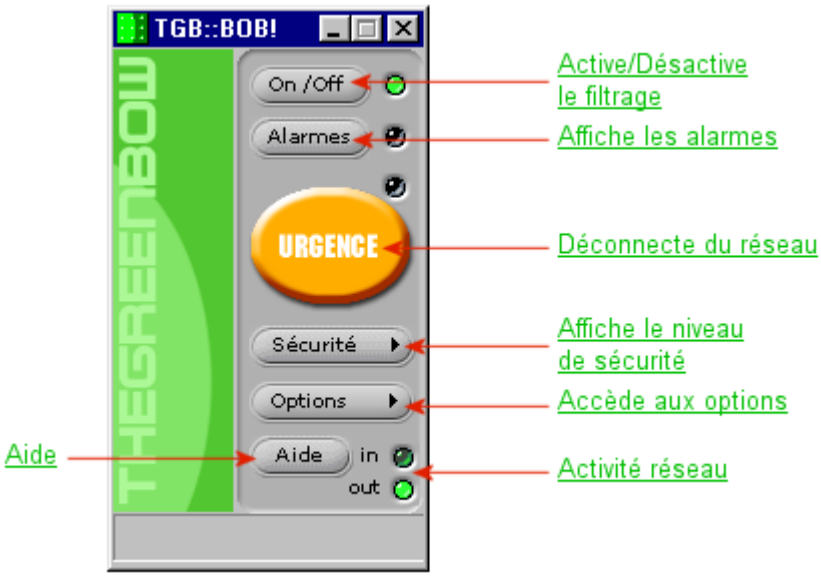
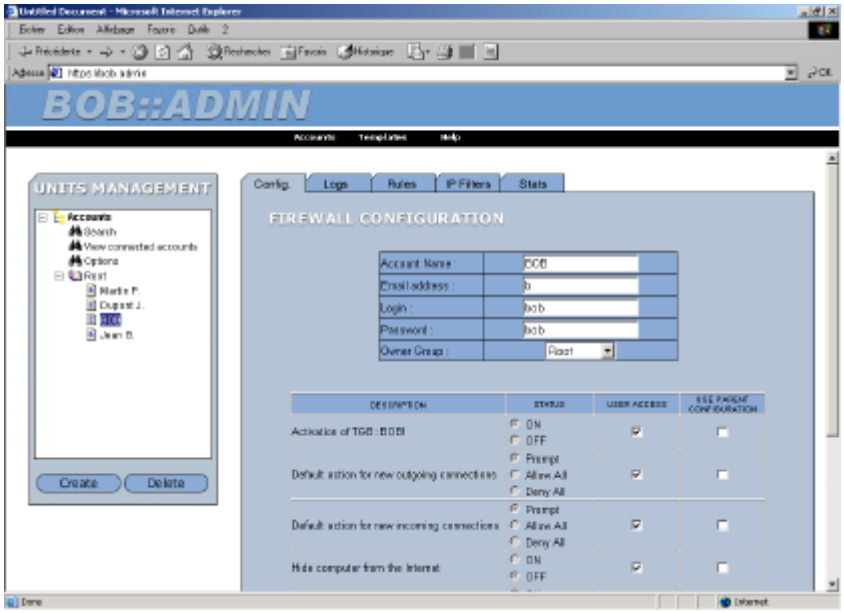


Fig. 3 Interface du firewall personnel

3.2 Serveur d'administration

BOB::ADMIN est le serveur d'administration de la solution TGB::BOB! Pro.



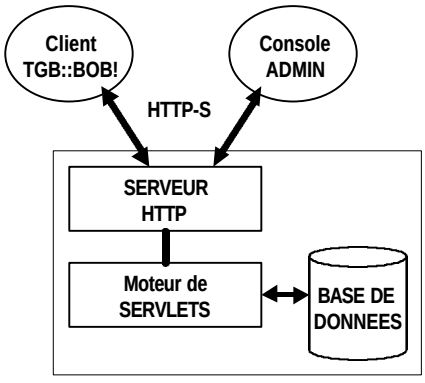
BOB::ADMIN permet la gestion du parc de firewalls personnels installés, la configuration des règles de sécurité de ces firewalls, indépendamment ou par groupe, la compilation des logs et des alarmes de chaque firewall.

Alors que l'ergonomie des firewalls personnels permet une utilisation quotidienne du logiciel par des néophytes, BOB::ADMIN offre à l'administrateur des possibilités de configurations plus complexes, communes à la configuration de firewalls classiques, comme par exemple les filtrages sur des adresses IP ou des ports spécifiques.

BOB::ADMIN permet ainsi de définir une politique de sécurité globale qui peut être imposée pour tout ou partie aux utilisateurs finaux, sans que ceux-ci ne soient perturbés dans leurs habitudes de travail.

Pour assurer une compatibilité maximale avec les ressources existantes de l'entreprise, BOB::ADMIN est bâti sur un ensemble de technologies standards :

- un serveur HTTP (Apache),
- un moteur de servlets (Jakarta-tomcat),
- une base de données (MySQL) qui permet l'exploitation des logs par n'importe quel outil classique de gestion de base de données,
- un protocole de communication HTTP et HTTP-S qui garantit la meilleure compatibilité avec les équipements réseau déjà opérationnels.



4 Installation et configuration

La simplicité intrinsèque de la solution a été portée jusqu'aux opérations d'installation et de désinstallation :

4.1 Firewall personnel

L'installation des firewalls personnels est une installation Windows standard. Elle peut être réalisée localement sur le poste à protéger, ou être distribuée suivant les procédures en vigueur chez le client (distribution de master, distribution et lancement de logiciels, etc…)

En mode "administré", l'installation du firewall personnel inclut le paramétrage de l'identifiant/mot de passe du firewall, et de l'adresse (IP ou DNS) du serveur d'administration.

4.2 Serveur d'administration

Afin d'éviter à l'utilisateur d'avoir à installer le serveur d'administration, et afin d'assurer la meilleure sécurité possible de ce serveur, celui-ci est fourni pré-installé sous forme de boîte noire.

Le serveur fourni est un PC, équipé de Linux ou de Windows 2000, sur lequel sont installés et pré-configurés un serveur HTTP, une base de données MySQL, un moteur de servlets.
Ce PC est équipé d'une interface Ethernet qui permet sa configuration depuis un poste connecté au réseau d'entreprise.

Option : La solution est aussi installable sur une machine du client. Cette installation "sur site" du serveur d'administration comprend l'installation des outils nécessaires à son fonctionnement (serveur HTTP, base de données, moteur de servlets, etc…) et la configuration, en terme de sécurité, de la machine hébergeuse.

5 Fonctionnalités

5.1 Firewall personnel

- Protection totale contre les intrusions, le vol de données et les attaques (chevaux de Troie, dénis de service...)
- Protection contre les scans d'IP et les scans de ports

- Contrôle des applications sortantes et des connexions entrantes
- Signature MD5 des applications filtrées
- Contrôle de conformité des paquets de données entrants avant leur transmission à l'O.S.
- Contrôle des communications entrantes IP et NetBIOS.
- Technologie avancée de suivi des connexions (stateful inspection)
- Mode "poste invisible"

- Facile à installer et à paramétrer (configuration par auto-apprentissage)
- Création des règles de filtrage "à la volée"
- Mode de filtrage : autoriser, avertir, interdire, mode "serveur"
- Possibilité de protéger la configuration par mot de passe
- Possibilité de couper le réseau en un clic (bouton "Urgence")
- Possibilité de couper le réseau automatiquement après un délai d'inactivité
- Supporte ICS (Internet Connection Sharing = Partage d'accès Internet)

- Création de journaux d'événements (fichiers logs) : alarmes, historique
- Visualisation en temps réel des connexions ouvertes
- Aide en ligne contextuelle et graphique

TGB::BOB! fonctionne avec tout type de connexion : réseau local, ADSL, Câble, Modem.
Configuration requise : PC, Windows 9x, Me, NT, 2000 ou XP

5.2 Serveur d'administration

- Centralisation de la configuration des postes équipés du firewall TGB::BOB!
- Gestion des postes nomades et administration multi-sites
- Centralisation et exploitation des logs par groupe ou par utilisateur
- Gestion centrale des règles de sécurité
- Possibilité de verrouillage des règles autorisées ou interdites
- Limitation de l'accès à toute ou partie de l'interface du firewall TGB::BOB!

- Visualisation en temps réel des postes connectés
- Gestion des comptes utilisateurs (création de groupes, création et suppression de comptes, etc…)
- Edition de modèles de règles
- Principe d'héritage des règles pour les utilisateurs d'un groupe
- Configuration complète des firewalls personnels
- Restriction d'utilisation de chaque firewall personnel
- Création de règles de filtrage IP (adresses IP, ports, direction, protocole, etc…)
- Communication sécurisée en HTTP-S entre les firewalls TGB::BOB! et le serveur BOB::ADMIN
- Communication sécurisée en HTTP-S entre la console d'administration et le serveur BOB::ADMIN

- Interface WEB accessible depuis n'importe quel navigateur

BOB:ADMIN est fourni sous forme de boîte noire pré-configurée, connectée au réseau d'entreprise.