

**deny all annonce son firewall applicatif rFTP
(remote-FTP) :
rFTP assure la protection
des serveurs FTP des entreprises.**

Paris, Février 2004

Le **File Transfer Protocol** (protocole de transfert de fichiers) ou **FTP** est dédié à l'échange informatique de fichiers sur un réseau TCP/IP.

En complément des applications traditionnelles issues des PGI ou autres systèmes de gestion, de nombreuses informations sensibles voire confidentielles (virements, factures, propositions, rapports confidentiels...) sont transmises sous forme de fichiers. Ces derniers sont stockés dans des répertoires sur des sites FTP, communément appelés des **serveurs FTP**.

FTP obéit à un modèle client-serveur, c'est-à-dire que l'une des deux parties, le *client*, envoie des requêtes auxquelles réagit l'autre partie, appelée *serveur*. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou une ligne de commande).

Le protocole, qui appartient à la couche application du modèle OSI, utilise une connexion TCP.

Il peut s'utiliser de deux façons différentes :

- en mode *actif*, les commandes et les réponses du serveur sont échangées sur le port 21 (*ftp*) selon le protocole Telnet, tandis que les données passent par le port 20 (*ftp-data*),
- en mode *passif*, seul le port 21 (*ftp*) est utilisé pour les commandes et données.

L'usage de ces deux ports est standardisé. Ils sont réservés aux connexions FTP. De ce fait, les firewalls classiques se contentent d'autoriser ou d'interdire les flux FTP sans en analyser les contenus.

Afin de sécuriser les accès Internet aux serveurs FTP internes à l'entreprise, **deny all** a développé **rFTP** : un produit dédié à la protection des serveurs FTP des entreprises.

rFTP est basé sur une technologie de type reverse-proxy optimisée et permet de :

- gérer de façon transparente le chiffrement SSL,
- filtrer la totalité des flux entrants FTP (commandes et données),
- centraliser les contrôles d'accès,
- sécuriser l'utilisation des serveurs FTP en les protégeant des failles et des dénis de services.

rFTP est composé de deux éléments complémentaires qui peuvent être installés sur des systèmes différents :

- le **Reverse FtpD** (RFD) : reverse proxy FTP,
- le **Secure Filtering Proxy** (SFP) : filtrage et centralisation des contrôles d'accès.

Reverse FtpD

Le composant RFD est l'interface avec les clients FTP. Il relaie les commandes et les données aux serveurs FTP de l'entreprise en évitant de les exposer directement.

Il permet par ailleurs de :

- gérer le chiffrement SSL (FTP/TLS)
- maîtriser au niveau applicatif les modes *passif et actif* (PASV ou PORT),
- gérer les différents time out,
- stocker les logs au format CLF de l'ensemble des requêtes utilisateurs,
- gérer le nombre maximum d'utilisateurs connectés simultanément,
- contrôler la conformité des lignes de commandes et des noms de fichiers envoyés.

Secure Filtering Proxy

Le composant SFP assure le filtrage de la totalité des flux FTP (commandes et données) à destination des serveurs FTP de l'entreprise.

Le SFP inclut notamment :

- le support centralisé des authentifications qui peut rester transparent si elles sont gérées par chaque serveur FTP.

Les authentifications suivantes sont supportées :

- RSA/SecurID, en s'appuyant sur un serveur RSA/ACE d'authentification,
 - user/password, en s'appuyant sur un annuaire LDAP pour l'authentification et l'habilitation ou sur des fichiers ASCII (utilisateur / mot de passe),
 - user/password FTP «anonymous».
- le filtrage qui permet de détecter et d'éviter :
 - Les attaques connues contre tout serveur FTP (failles et dénis de service),
 - Les tentatives d'utilisations abusives des commandes FTP.

- le moteur de filtrage qui intègre les fonctionnalités suivantes :
 - Réécriture des chemins d'accès pour la mise en cage,
 - Contrôle des fichiers entrants possibles avec les modules externes (anti-virus, type, contenu,...),
 - Filtrage intégral des commandes et des données entrantes.

L'ensemble des fonctionnalités de rFTP est administrable au travers d'un navigateur.

A propos de deny all

deny all est un éditeur français de solutions de sécurité informatique. Spécialiste de la sécurité applicative, son offre comprend des solutions disponibles sous forme logicielle ou appliance. Les solutions **deny all** répondent à des enjeux stratégiques tels que l'ouverture des systèmes d'information aux collaborateurs, fournisseurs, clients et partenaires de l'entreprise.

deny all, a été créée en 2001 avec une équipe d'experts en sécurité. Ses solutions de sécurité applicative bénéficiaient déjà de plusieurs années de développement puis de mise en production au sein de grandes entreprises.

Aujourd'hui, **deny all** commercialise ses solutions dans le monde entier et protège plusieurs centaines de sites Web en France, en Europe, aux États-Unis et en Asie grâce à ses différents produits rWeb, rFTP et sProxy.

RELATIONS PRESSE

Pour tous renseignements complémentaires, vous pouvez contacter :

Information Société	Information Presse
<p>deny all</p> <p>Marie-Josée SPINOSI</p> <p>5, rue Scribe</p> <p>75009 PARIS</p> <p>Tél : 01 40 07 47 19</p> <p>Fax : 01 40 07 47 27</p> <p>Email : mjspinosi@deny-all.com</p> <p>www.deny-all.com</p>	<p>ITGS PR</p> <p>Laëtitia BERCHE, Bernard MOAL</p> <p>15, rue d'Estienne d'Orves</p> <p>92130 Issy-les-Moulineaux</p> <p>Tél : 01 58 88 39 58</p> <p>GSM : 06 14 48 02 95</p> <p>Email : lberche@itgspr.fr</p> <p>www.itgs.net</p>