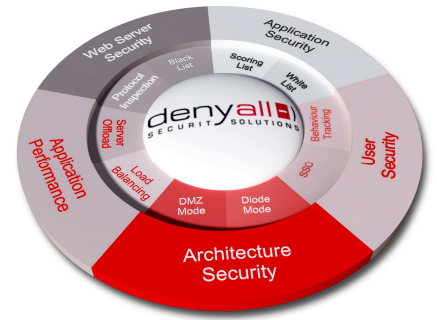


rFTP 3.0

File Transfer Application Firewall



rFTP, protection of FTP servers and file transfers

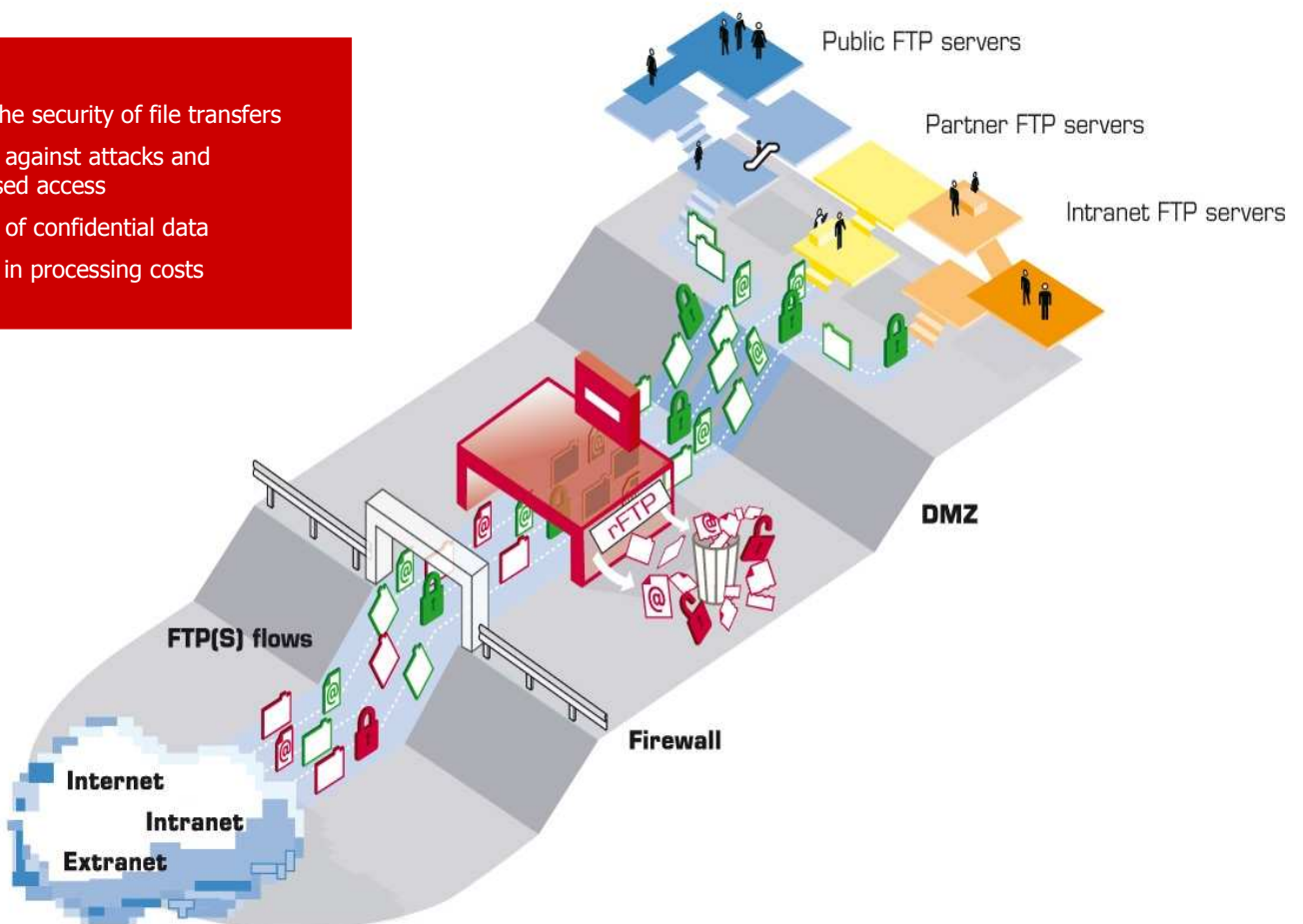
- Integrates filtering of FTP requests
- Fast, simple implementation of secure File Transfer (FTP/SSL)
- Centralised user authentication
- Strengthened access control
- Content checking of uploaded files

Transferring data files by FTP has enormously improved organisations' efficiency and user productivity when compared with previous methods; EDI (Electronic Data Interchange), fax or reliance on postal services. Established and proven, the FTP protocol alone, however, does not provide sufficient security to enable it to be used more widely.

The rFTP solution – remote FTP – guarantees the highest level of protection to both servers and data transfers in FTP mode. It thus protects organisations against risks of security flaws which can lead to confidential information theft, industrial espionage and damage to company image. With rFTP, organisations have at their disposal a file transfer infrastructure that is efficient, upgradeable and secure.

Benefits

- Ensuring the security of file transfers
- Protection against attacks and unauthorised access
- Protection of confidential data
- Reduction in processing costs



Technical characteristics

Based upon an optimised reverse proxy technology, the rFTP application firewall filters entirely the data flow exchanges, encrypted or not, with all of an organisation's FTP servers.

It makes file transfers secure through the swift implementation of FTP/SSL whilst simplifying infrastructure and reducing processing costs through the use of standard FTP.

Complete protection of FTP servers

Making use of a positive security model, rFTP authorises only those file transfers conforming to normal usage.

It immediately blocks :

- attempts to exploit server weaknesses
- unauthorised access
- erroneous user requests

Normal usage rules are predefined in rFTP. They can be refined to determine precisely the rights by user and by server (downloading, file or directory deletion or renaming,...).

Benefits :

- protection against theft of sensitive data
- intrusion prevention
- reduction in the costs of "fixing" software

Fast implementation of secure File Transfer (FTP/SSL)

rFTP ensures client authentication and guarantees the confidentiality and conformity of data exchanged between clients and servers.

The deployment of authentication and the decryption of the data flow is achieved quickly and with no impact on the infrastructure, firewalls and servers already in place (RFC4217 supported).

rFTP centralises :

- user authentication :
 - ▶ X509 SSL/TLS certification
 - ▶ RSA SecurID
 - ▶ User/Password by LDAP server
- SSL/TLS encryption up to 256 bits.



Access Control

rFTP authorises a granular access control by :

- User
- access profile: write, enquiry only...
- access perimeter: access limited to directories and files only to which the user is authorised
- maximum number of users

Control of uploaded files

- maximum permitted size of transmitted files
- content and format checking by calling up Third Party software (antivirus,...)

Protection of confidential data

rFTP validates and filters the filenames and extensions of outgoing data. It thereby blocks even unintentional transmission of company confidential information.

Infrastructure simplification

- deployment compatible with all types of firewall due to compliance with active and passive FTP modes
- transparent implementation of authentication and secure FTP/SSL transfers
- centralised authentication and access control

Ease of administration

- Web graphic interface remotely accessible in secure mode
- several administrator access profiles
- access logs and statistics and application filter results (exportable)

rFTP, Interoperability and Performance

- Available as an open appliance or as software only
- Transparent integration
- Fully compatible with all leading browsers, firewalls, FTP servers, load balancers, and statistical tools
- Over 1000 simultaneous file transfers on a single appliance
- High Availability architecture deployment

Deny All is member of SAP Global Security Alliance, CLUSIF, l'OSSIR, l'OWASP and Associate Member of the Liberty Alliance.

**Find Deny All
in the world on :**

www.denyall.com

Deny All resolves the content problem, the principal medium for attacks over recent years, with its range of proactive application control and flow acceleration solutions

Contact

info@denyall.com
Tel : +33 (0)1 40 07 47 14
Fax : +33 (0)1 40 07 47 27
23, rue Notre Dame des Victoires
75002 Paris - France