



Druvaa inSync – Security Overview

© Druvaa Software 2008 | April 2008

The document gives an overview of Druvaa inSync and discusses the architecture from features from a security standpoint.

Druvaa inSync – Overview

Druvaa inSync is an enterprise class product for secure and continuous synchronization of your critical data from laptops and desktops to a central enterprise server over LAN or WAN.

Druvaa inSync is an ideal solution for increasing personal data availability for improved business continuity and recovery. The light weight inSync client non-intrusively and non-disruptively monitors changes to critical data and *securely* syncs the delta changes to a central enterprise server.

The powerful features like bandwidth scheduler and WAN optimizer makes it ideal for traveling enterprise users who don't have a secure and dedicated connectivity to office servers.

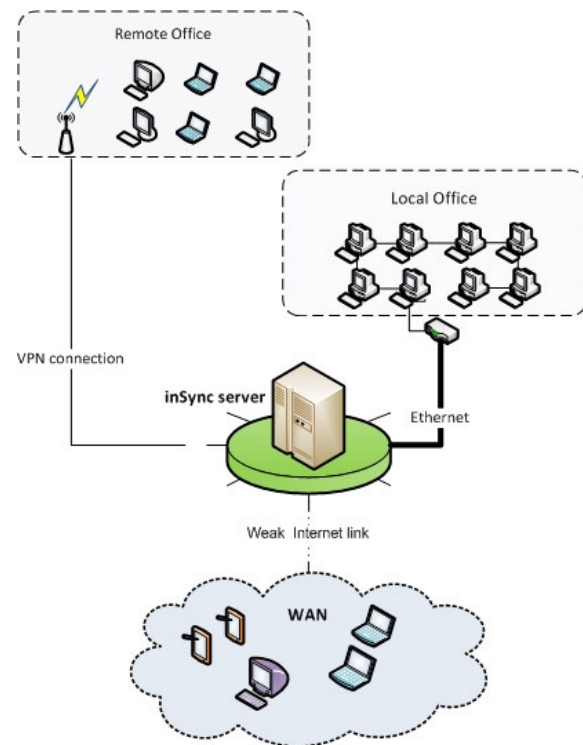
Due to insecure nature of WAN, the corporate data cannot be simply trusted on it. This document discusses the advance security features in Druvaa inSync which make backup and restore bulletproof. **Client triggered backups** and **SSL encryption** make sure that the data is always secure on wire and **advanced authentication** system and **on-server encryption** make sure even the administrator cannot tamper the data.

Druvaa inSync Architecture

Druvaa inSync architecture consists of two components –

1. light-weight Druvaa inSync client and
2. Druvaa inSync enterprise server.

The diagram below shows a Druvaa inSync installation –



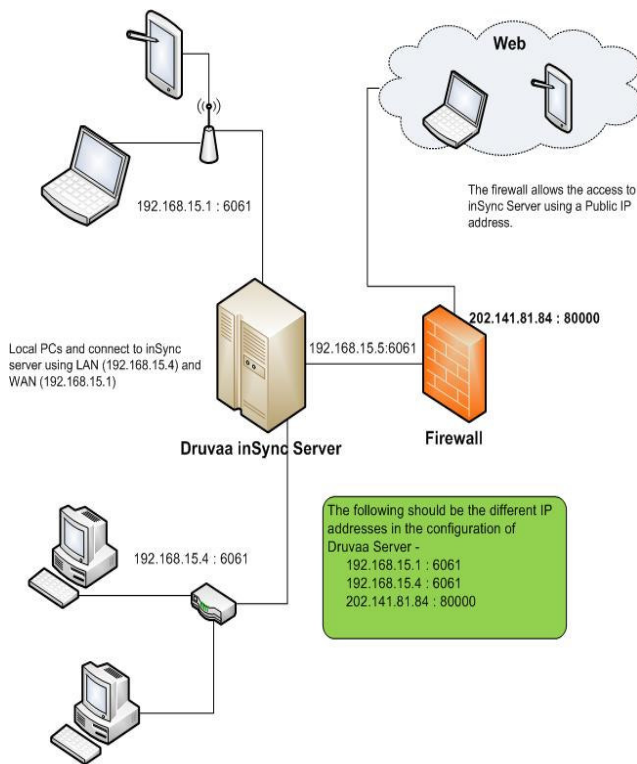
A host based soft driver is equipped with sufficient backup intelligence to initiate and accomplish backup. The inSync client continuously monitors and captures file level updates on configured files and folders, creates compressed delta patches and asynchronously replicates them securely to Druvaa inSync Enterprise Server over LAN/VPN/WAN.

Client Triggered Backups

Most administrators do not put the backup server in *demilitarized zones* (DMZs) as they are afraid of out-bound sockets and data flowing through them.

With Druvaa inSync the backup and restore requests are always initiated by the inSync client, which aids in security and scalability of the inSync server. Also, both backup and restore just use same (default 6061) port for all configuration, control and data request.

Which means the admin just expose a single inbound (ALL to 6061) port on the backup server. The following figure shows the Druvaa inSync server configuration -



Secure Client Authentication

On every client creation the server sends out a inSync key file (.isk) file, which contains the server information and 32 bytes unique authentication credentials for the client.

Starting version 2.0, after the first connect the client re-negotiates the authentication parameters. And whenever the key is re-generated by the administrator, the in-use key is reset and the connecting user sees - "Expired Key" message. This ensures that the user data never lands in hands of malicious user.

256 Byte SSL On-Wire Security

To protect the corporate data on unsecured internet, Druvaa inSync provides strong on-write 256 byte SSL encryption. On installation the server publishes self signed SSL X509 certificates which the client validates and uses for SSL every time it connects. This ensures bulletproof on-write security.

Encrypted data on Server

Druvaa inSync Enterprise server (starting ver. 2.0) optionally encrypts the data stored on the server using highest US govt. standards of AES (Advanced Encryption Standard) encryption.

Druvaa inSync server also goes one step further by generating the AES key on-demand during the server installation. This breaks the dependency on any statically generated key.

Summary

This document demonstrates, Druvaa inSync provides highest standards of security and data protection using advances standards of authentication, authorization and data encryption. This enables secure backups and non-intrusive restores.