



Druva inSync – Security Overview

© Druva Software 2010 | September

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

Druva inSync – Overview

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

Druva 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.

Powerful features like the *Bandwidth Scheduler* and *Octopus WAN Optimization Engine* make it ideal for traveling enterprise users who don't have secure and dedicated connectivity to office servers.

Due to the precarious nature of WAN, corporate data cannot be simply trusted on it. This document discusses the advance security features in Druva 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** ensure that even the administrator cannot tamper the data.

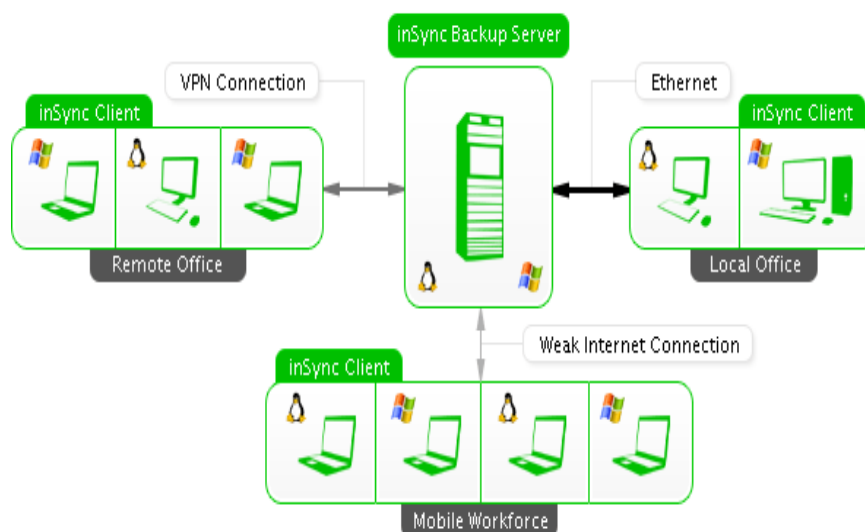
Druva inSync Architecture

Druva inSync architecture consists of two components –

1. Light-weight Druva inSync client and
2. Druva inSync enterprise server.

The diagram shows a Druva 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 Druva inSync Enterprise Server over LAN/VPN/WAN.

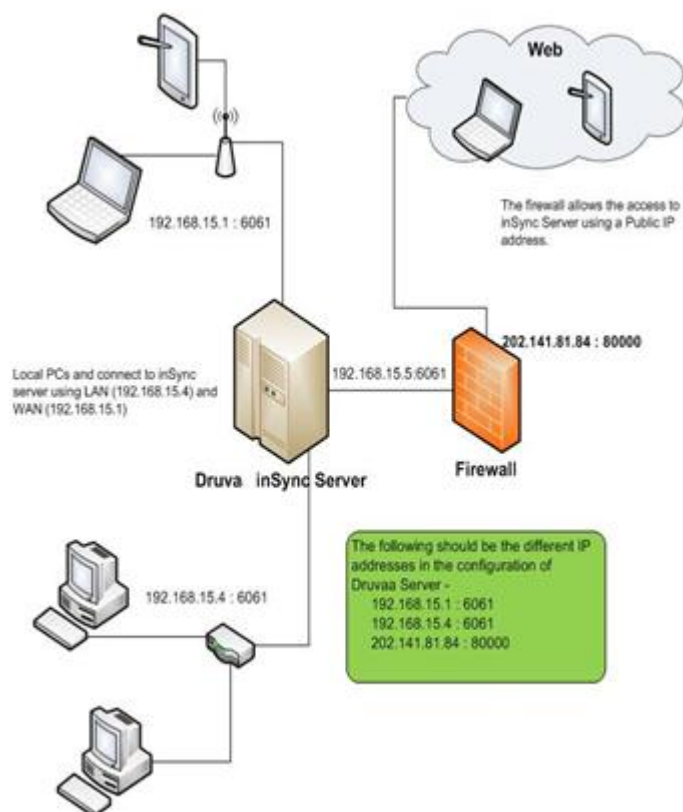


Client Triggered Backups

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 Druva 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 the same (default 6061) port for all configuration, control and data request.

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



Secure 32 Byte 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.

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 Bit SSL On-Wire Security

To protect the corporate data on unsecured internet, Druva inSync provides strong on-write 256 bit 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.

256 Bit Storage Encryption

Druva inSync Enterprise server encrypts the data stored on the server using highest US govt. standards of AES (Advanced Encryption Standard) encryption. The data in the storage is encrypted using 256 bit strong AES encryption.

Run-Time Key Generation for Better Security

Druva inSync server goes one step further by generating the SSL and AES keys on-demand during the server installation. This breaks the dependency on any statically generated keys, and enhances the security

The SSL key can later be replaced by a fully signed SSL certificate by any official signatory.

The Blackbird Storage Engine

The Blackbird storage engine stores the backed up data in 1024 ISD (InSync Data) files. It uses data deduplication to break the user backup files into small (8KB or less) blocks and store them in different ISD files. This makes it nearly impossible for anyone to assemble the user files again, without the complete knowledge of file's original construct and Blackbird's proprietary file format.

Summary

This document demonstrates that Druva inSync provides highest standards of security and data protection using advanced standards of authentication, authorization and data encryption enabling secure backups and non-intrusive restores.

About Druva

Druva provides premium enterprise class solutions for data protection and disaster recovery. The products make an intelligent use of Continuous Data Protection and Data deduplication technologies to bring a paradigm shift in an enterprise's approach towards data protection.

With key technological advancements, the data protection solutions deliver up to 90% better bandwidth and storage utilization compared to the traditional methods. This ensures faster and smoother backups especially for remote laptops, mobile users and distant servers.

For more information please refer to the website at - www.Druva.com