

NCI Offsite Data Backup White Paper



Data Security

Table of Contents

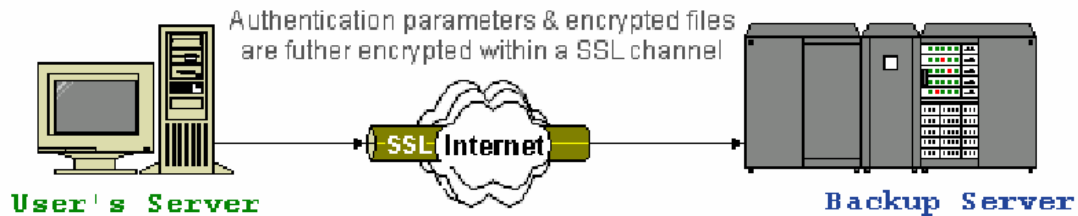
TABLE OF CONTENTS	2
1 INTRODUCTION	3
2 OFFSITE DATA BACKUP – “SECURE, ROBUST AND RELIABLE”	4
2.1 SECURE 128-BIT SSL COMMUNICATION	4
2.2 BACKUP DATA SECURELY ENCRYPTED	4
2.3 WE DON’T KEEP YOUR ENCRYPTING KEY	5
2.4 BEST ENCRYPTION ALGORITHM IS USED	5
2.5 REQUIRE 1.99×10^{16} YEARS TO CRACK THE 128-BIT ENCRYPTION	5
2.6 RESTRICT ACCESS TO DATA BY IP ADDRESSES	5

1 Introduction

This document describes the security measures available in Offsite Data Backup software from the user's perspective. It serves as a reference for partners when addressing customers' queries on security.

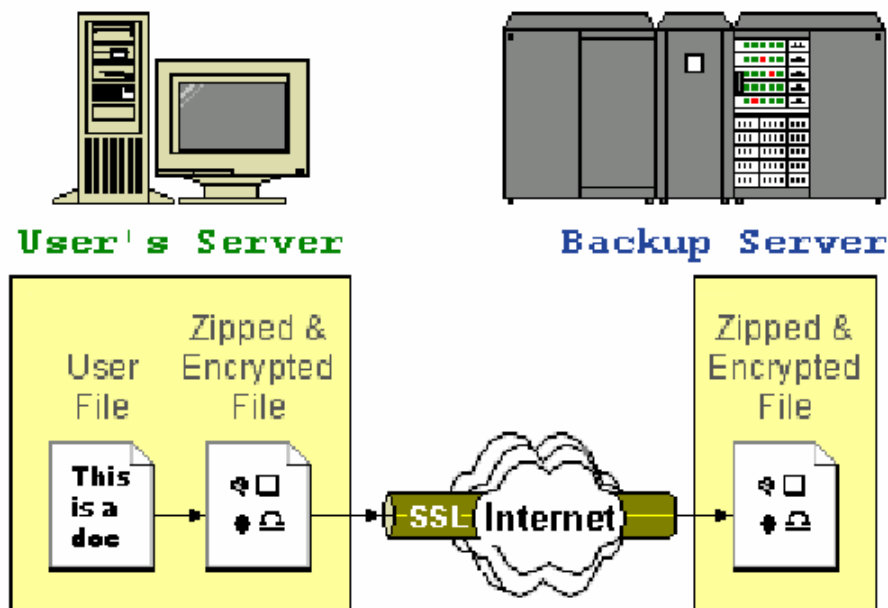
2 Offsite Data Backup – “Secure, Robust and Reliable”

2.1 Secure 128-bit SSL communication



All communications between Offsite Data Backup and your computer are transported in a 128-bit SSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (internet), eavesdroppers have no knowledge of what has been exchanged.

2.2 Backup data securely encrypted



All of your files are first zipped and encrypted with your defined encrypting key before they are sent to Offsite Data Backup. To all people but you, your files stored on Offsite Data Backup are no more than some garbage files with random content.

2.3 We don't keep your encrypting key

The encryption key used to encrypt your files resides only on your computer and is known only to you. It is never transmitted anywhere across the network. If this key is lost, all backup files can never be recovered. Therefore, although we have access to all files you stored on our backup server, we have no knowledge of the content of the files you stored.

Reminder: Please make sure you write down your encryption key in a safe place where it will never be forgotten. Otherwise, you will never be able to recover your backup files.

2.4 Best encryption algorithm is used

Currently, the algorithm that we are using to encrypt your files is 128-bit Twofish. It is a block cipher designed by Counterpane Labs. It was also one of the five Advanced Encryption Standard (AES) finalists chosen by National Institute of Standard and Technology (NIST). It subjects to frequent public reviews but no known attack against this algorithm has been reported.

2.5 Require 1.99×10^{16} years to crack the 128-bit encryption

A 128-bit key size has 2^{128} or around 3.4×10^{38} possible combinations. Even if you have the world's best supercomputer at 54 teraflops, it would take 8.77×10 years to test all combinations. Assuming it just needs one computer operation to test a possible combination, to use brute force attack (checking all combinations) on this encryption algorithm. It would take:

$$\frac{3.4 \times 10^{38}}{54 \times 10^{12}} \text{ seconds, or about } 6.3 \times 10^{23} \text{ seconds.}$$

That's about 199,654,245,823,702,952 years to successfully try all combinations. That's assuming that the supercomputer can test one combination per computer operation, which it can't. You can be sure that your data stored on our server is 100% secured.

Source: <http://tinyurl.com/oa2u9>

2.6 Restrict access to data by IP addresses

You can also restrict access to your backup files from the set of IP addresses you define. If someone tries to access your data from an IP address not on your defined list, their access will be denied. This additional security ensures backup files are not open to all locations even if the username and password are known.