Confidentiality, Integrity, Availability (CIA):

These are the three basic components of information security. Three primary goals of Network Security are Confidentiality, Integrity and Availability:

Confidentiality:

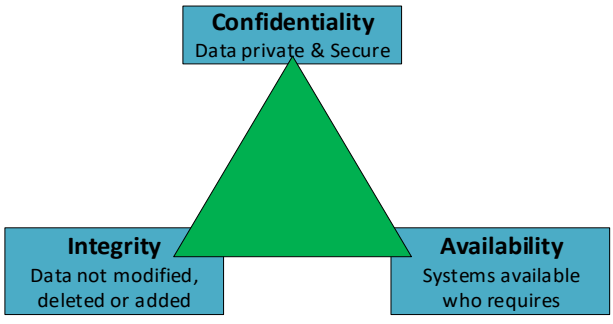
- The first goal of the Network Security or the Information Security is the “Confidentiality".
- Property that information is not made available or disclosed to unauthorized individuals.
- Function of "Confidentiality" is in protecting precious business data in Storage or in Motion.
- Function of confidentiality is protecting precious business data from unauthorized persons.
- It is part of Network Security make sure that data is available only to intended & authorized.
- Access to business data should be only for those individuals who are permitted to use data.
- Several ways to protect confidentiality of system or its data common is to use encryption.
- Encryption of data in transit with use of site-to-site & remote access virtual private network.

Integrity:

- The second goal of the Network Security or information Security is the "Integrity".
- Integrity aims at maintaining and assuring the accuracy and the consistency of data.
- Ability to make sure that a system and its data has not been altered or compromised.
- It ensures that data is an accurate & unchanged representation of original secure data.
- Integrity is to make sure that date is accurate & is not changed by unauthorized persons.
- The data received by the recipient must be exactly same as the data sent from the sender.

Availability:

- The third important goal of network security or information Security is the "Availability".
- The Systems, Applications, and Data must be available to authorized users when needed.
- The Systems, Applications, & Data must be available to authorized users when requested.
- Availability is to make sure Data; Network Resources are available to the legitimate users.
- The most common attack against availability is a Denial-of-Service (DoS) or DDoS attack.
- Safeguards that address availability include access controls, monitoring, data redundancy.
- Resilient systems, virtualization, clustering, environmental controls and incident response.



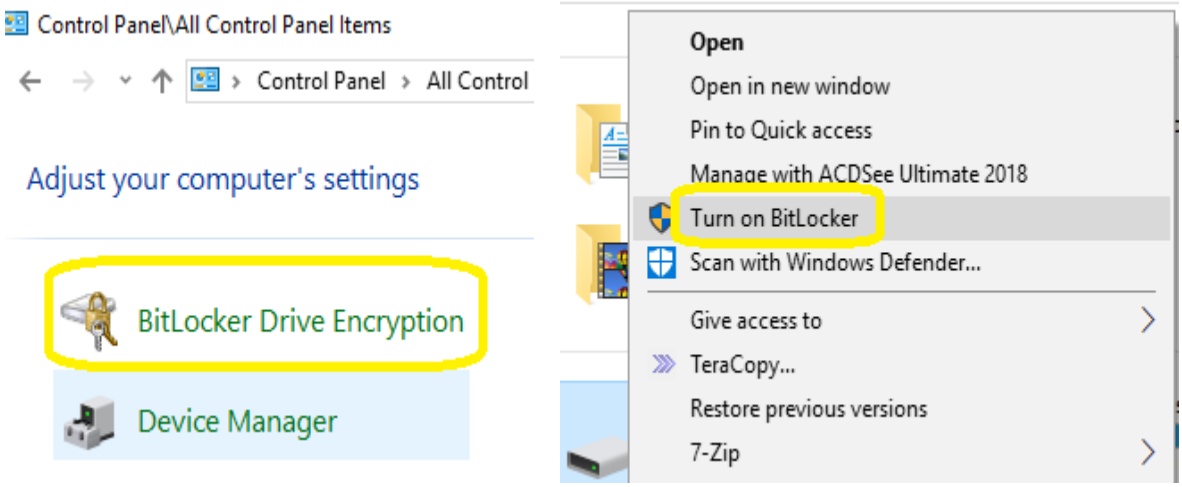
 Created by Ahmad Ali E-Mail: ahmadalimsc@gmail.com , Mobile: 056 430 3717

Confidentiality:

Encryption of Drive and Data:

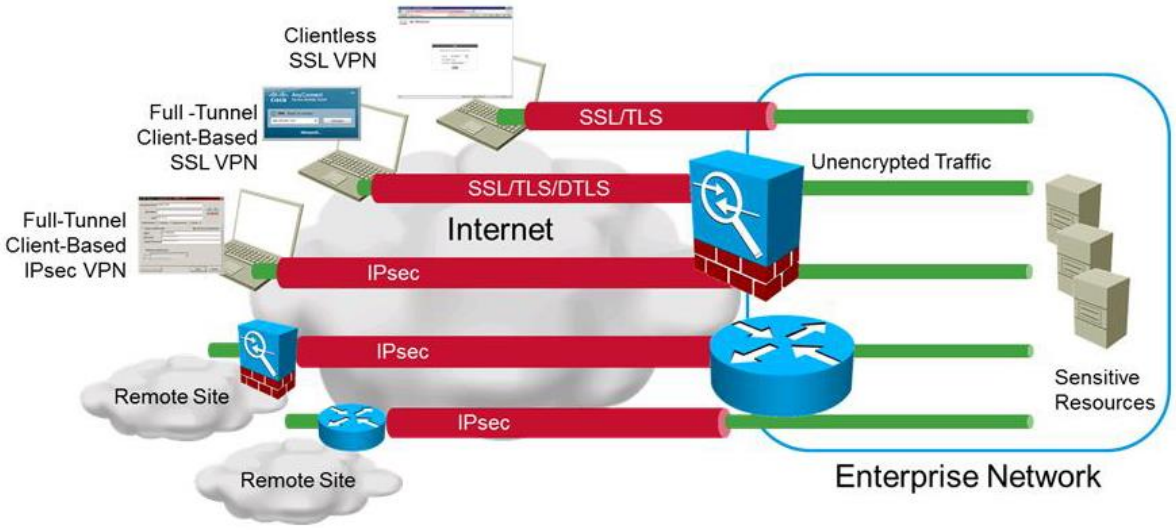
Using Window BitLocker Application:

Using Windows Pre-deploy application BitLocker. BitLocker can be used by right click in the given Window Drives and Turn on or from Control Panel going to BitLocker Drive Encryption and choose the drive to encrypt.



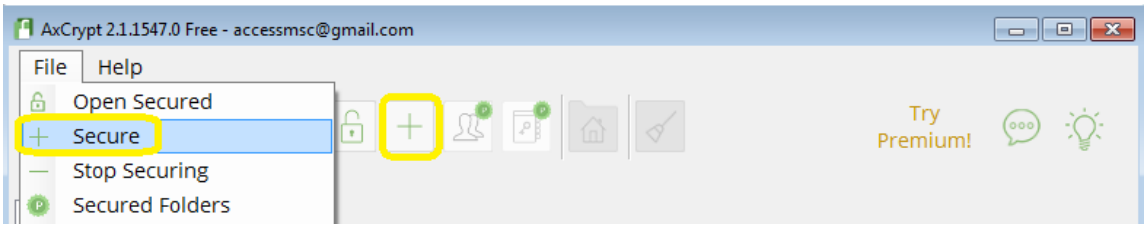
Encryption Transit Data:

Encryption of data in transit with use of Site-to-Site & remote access virtual private network.

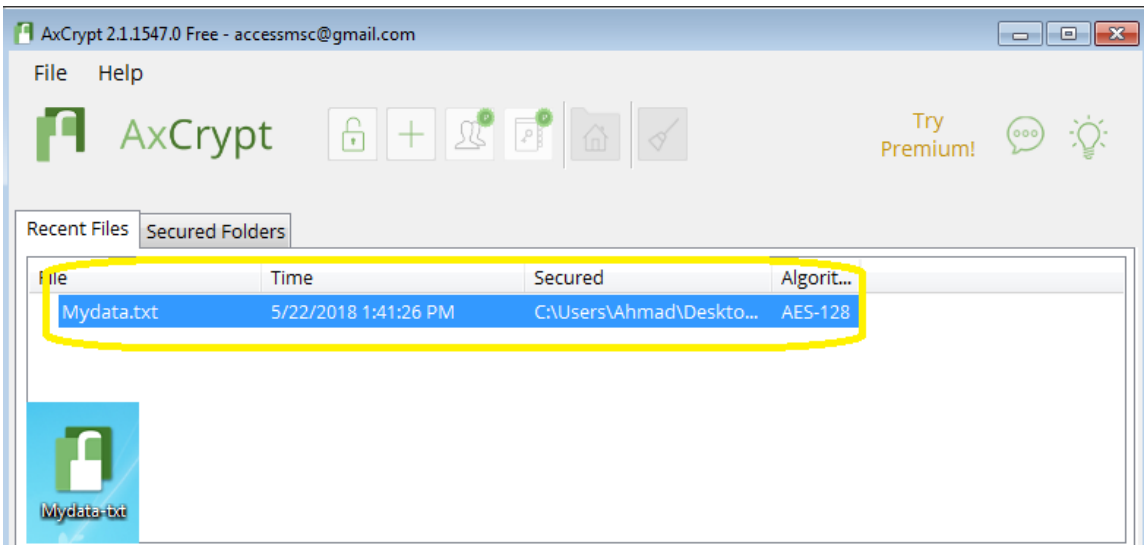


Third Party Tool AxCrypt:

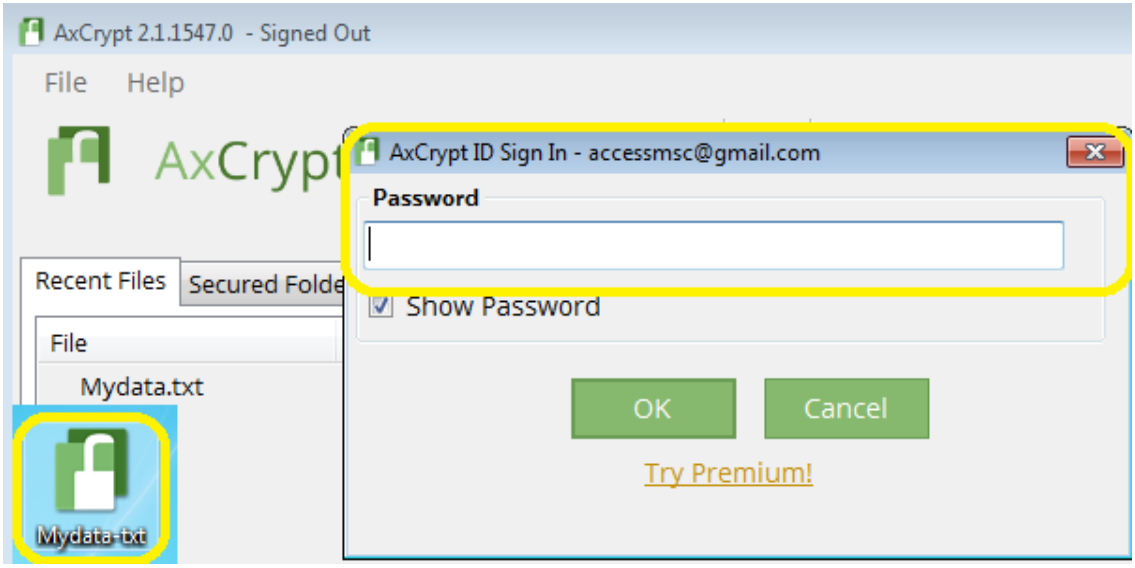
If BitLocker is not available in Windows, Linux or MAC systems, third Party tools can be used to encrypt files and drive. Such as AxCrypt first register Email and password for AxCrypt login then click on **Plus sign** on menu or **File Menu > Secure** Open the file to encrypt.



The open file **Mydata.txt** has been encrypted now.



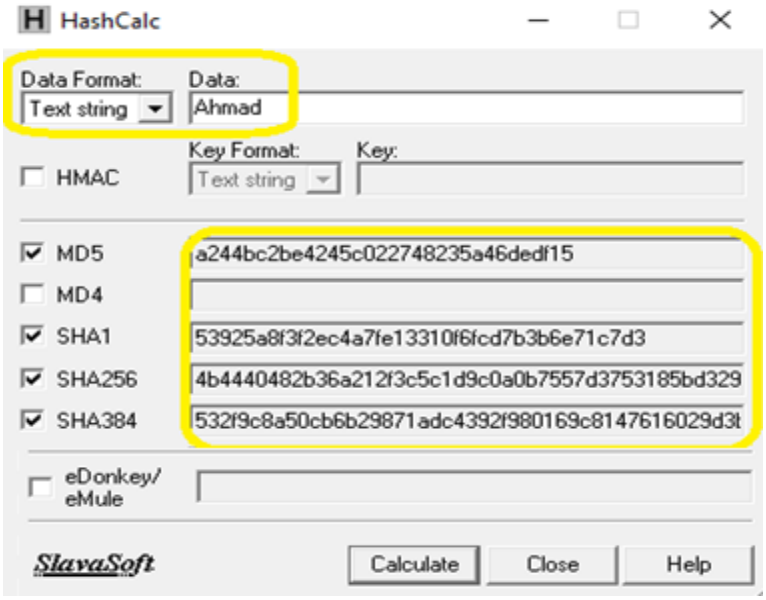
The encrypted data can only be open until type the correct email **password**.



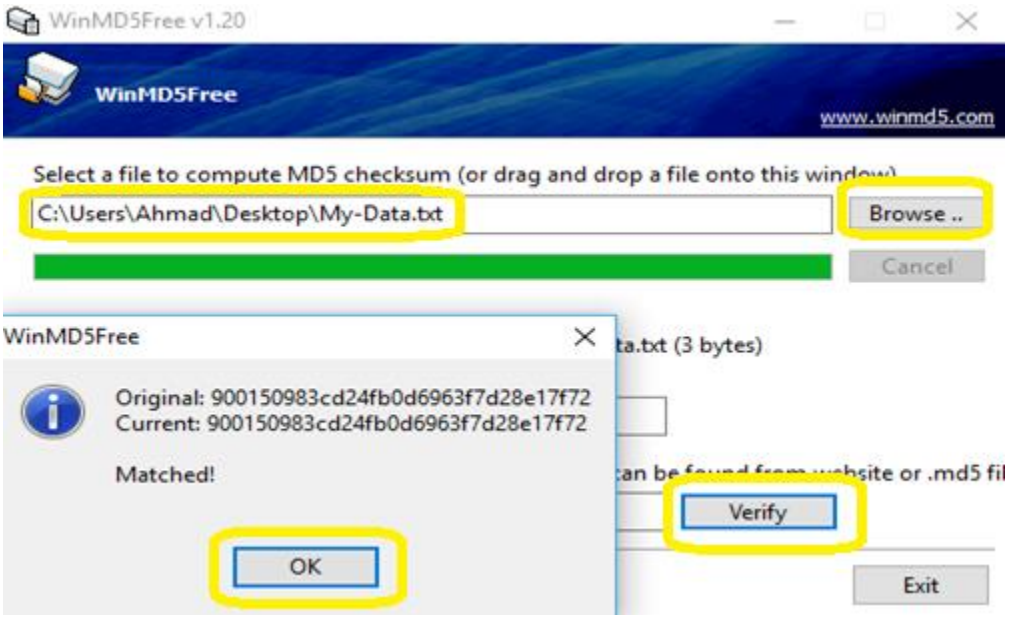
Integrity:

Hashing:

Open **HashCalc** change Data Format to **Text string** in Data: type any text as example I have type Ahmad. The **HashCalc** will generate Hash for the given Text string.

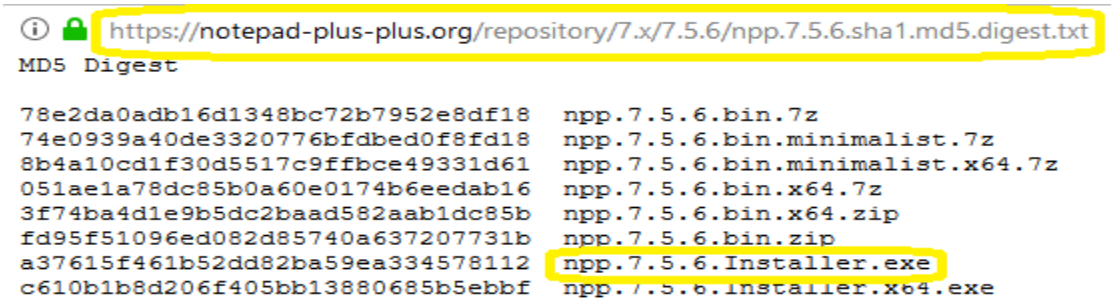


To check the integrity of any data file open WinMD5Free Application browse the file, it will show you the MD5 hash of the given file. Input the original MD5 hash in second bar and click Verify if the file is not corrupted it will show Matched.

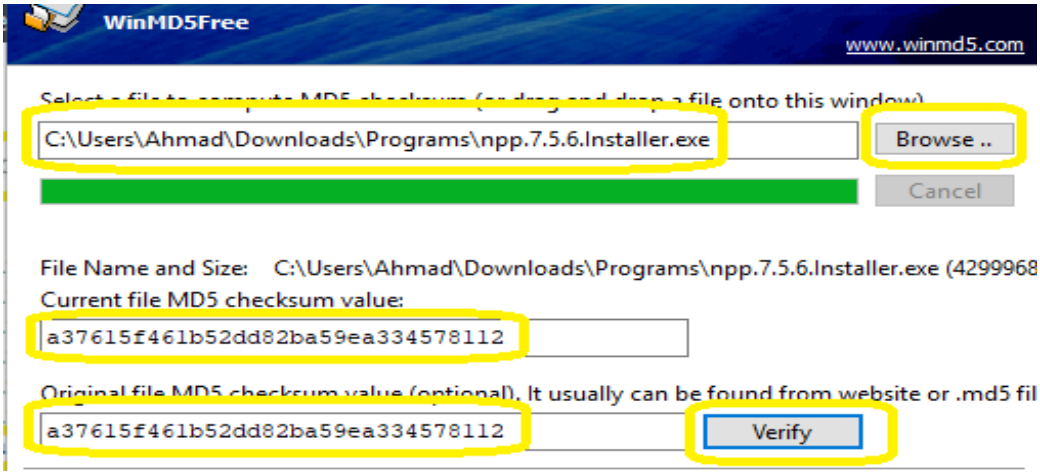


MD5 Hash is also used for Applications and Software integrity. Suppose go below link and download Notepad ++ application, the website have also given SHA and MD5 Hash Digest for check the integrity of application.

The given Application MD5 digest for cross checking.

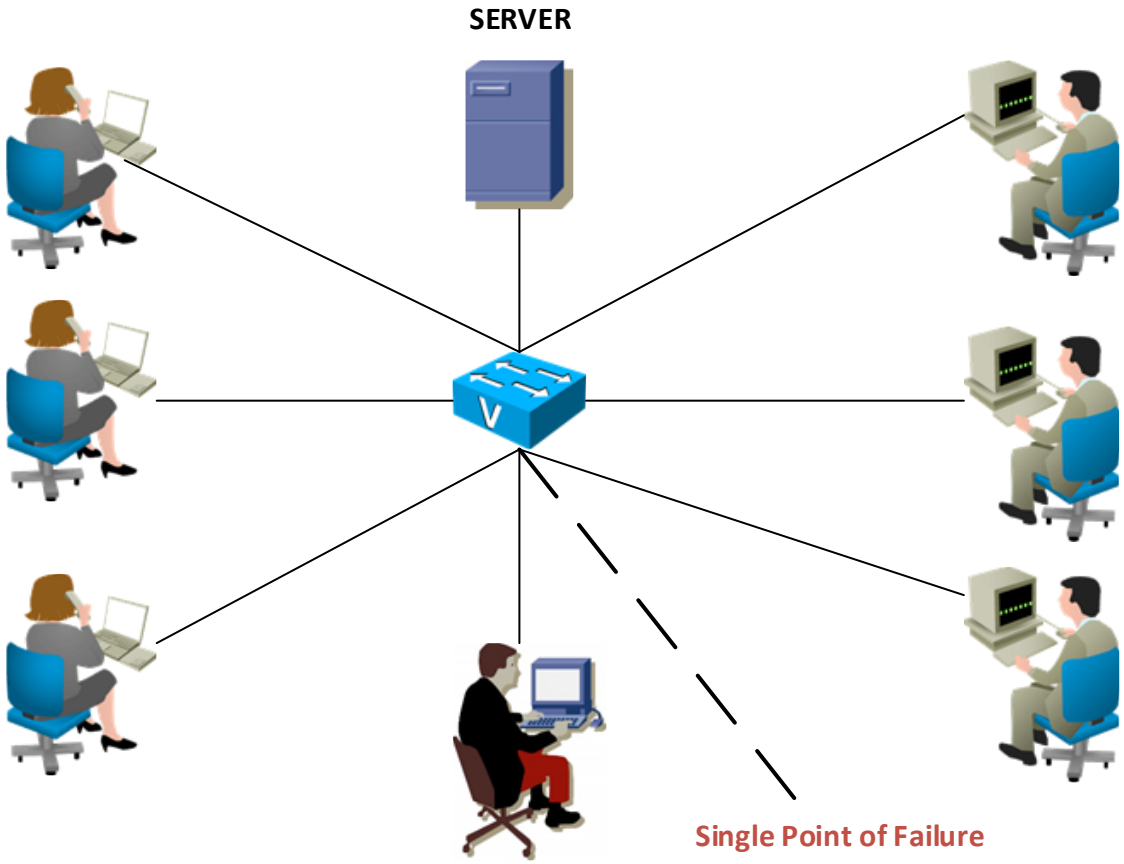


Open WINMD5Free Application browse the downloaded Notepad ++ application it will show the current MD5 Hash of the browse application cross check with above given MD5 Digest by click the Verify button. If Match it means the Notepad ++ is not corrupted or not modify for any third person. If not match, it means the application either is corrupted or has been modify by someone.

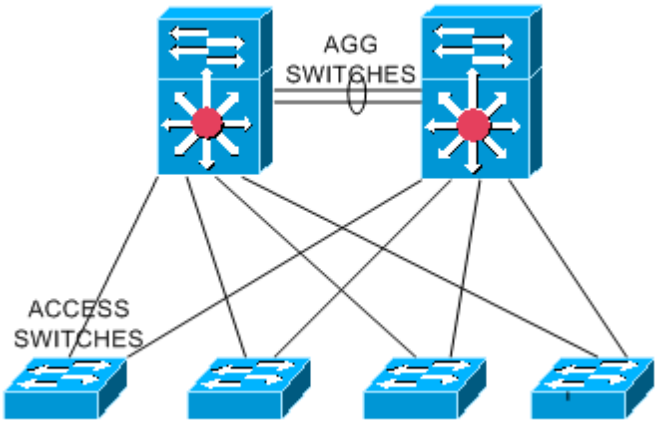


Availability LAB:

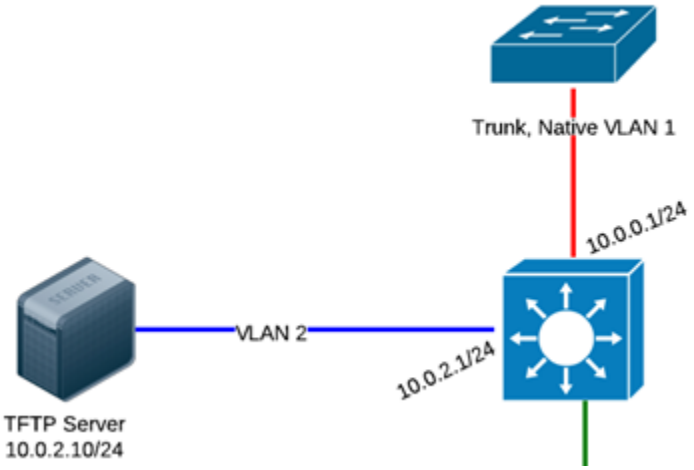
Single Point of Failure:



The above topology is Single point of Failure if the sever link or switch down no services will be available for any connected users. That why require **redundant switches** and **links**.

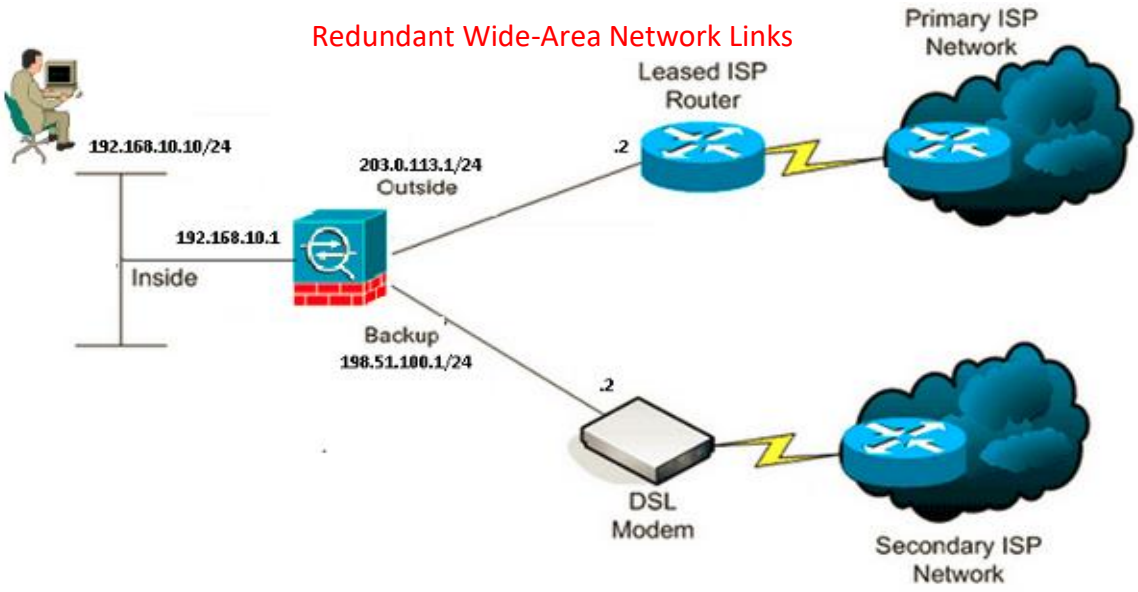


Backups:



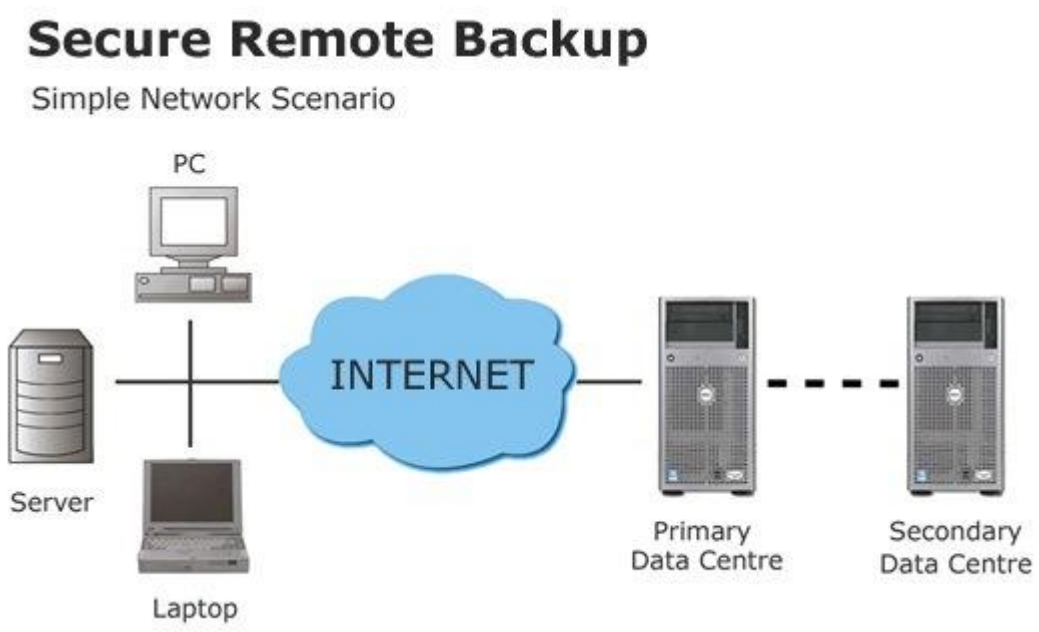
Redundancy:

Redundant Wide-Area Network Links



Redundant power supplies

Backup Systems:



Uninterruptable Power Supply

RAID Redundant Array of Independent Disks

Fault Tolerance: