Remote Management: Remote Desktop Connections

- Remote Desktop Services (formerly known as Terminal Services) allow a server to host multiple, simultaneous client sessions.
- Remote Desktop uses Remote Desktop Services technology to allow a single session to run remotely.
- RD helps theadministrator to manage the server using his own computer, without going to server room. This is done using Remote Desktop Protocol (RDP).
- If remote administration mode for the server is needed, the **Remote Desktop Services (RDS)** role in Windows Server is to be installed.
- Follow these steps to enable remote desktop access using Server Manager.

1) Logon to Windows Server as administrator and open Server Manager from the desktop Task Bar or Start Screen.
2) In the left pane of Server Manager, click Local Server.
3) Wait a few seconds for the information about the local server to update in the right pane. In the Properties section of the right pane you should see the status of Remote Desktop, which is disabled by default.
4) Click on the status to change it to Enabled. The Systems Properties dialog opens on the Remote tab. Under Remote Desktop in the Systems Properties dialog, select Allow remote connections to this computer and click OK.
5) By default, the administrator account has permission to access the server remotely. Optionally, you can also click **Select Users**… to give other users remote desktop access permission.

Remote Management: Remote Desktop Administration

- Remote Desktop for Administration is the default implementation of Remote Desktop Services (RDS) on a Windows Server 2012 R2 server.
- Here maximum two administrators can remotely log on to a server and do whatever they can do physically at the server.
- Limitation is that, when there is a reboot, system is disconnected.

Remote Management: Remote Desktop Assistance

- A method by which a remote user, say user A, accesses the desktop of another user, say user B, remotely and works on that desktop so that user B also can see the working.
- Remote assistance is used when you need or you wish to give some assistance remotely. The user has to give administration rights to the helper.
- Say you face a technical issue in your machine. The technical person whom you contact regularly can access your machine from the confines of his office remotely. This way you as well as the technical person are viewing the same screen. If you share your machine controls, then the technical guy can use your mouse to control your machine.
- In remote assistance, the user needs to be present to give access to the machine to the technical person unlike remote desktop.
- To use remote assistance, ther server needs to be installed with Remote Assistance role from AD Roles and Features.
- With the Remote Assistance feature added, Remote Assistance should now be enabled on the server. You can verify it with these steps:
  - Press the Windows key, right-click Computer, and select Properties from the taskbar.
  - Click Remote Settings and Verify that the “Allow Remote Assistance connections to this computer” check box is selected.
  - Click the Advanced button. Verify that the “Allow this computer to be controlled remotely” check box is selected.
- The default lifetime of invitations is six hours, but it can be changed. After the time limit has passed, the invitation can no longer be used to connect.

Remote Management: Remote Desktop Assistance...

- **Sending a Remote Assistance Request**
- The user who needs assistance should follow these steps to create a Remote Assistance request and begin the process:
  - Click Start, type *msra* in the Run box, and press Enter. The Windows Remote Assistance dialog box will appear.
  - Click “Invite someone you trust to help you.”
  - Click “Save this invitation as a file.”
  - Browse to a location on your hard drive. The invitation file is named *Invitation.msrcIncident* by default but can be changed if desired. Click Save.
  - A password is automatically created and can’t be changed. You’ll need to tell the helper this password.
  - Send the invitation to a helper as an email attachment, or place it on a share accessible to the helper.
- At this point, the person needing help must wait for the response from the helper.

Remote Management: Remote Desktop Assistance...

- **Responding to a Remote Assistance Request**
  - The helper can follow these steps with the person requesting assistance to begin a Remote Assistance session:
  - Double-click the invitation received from the person requesting help.
  - This invitation could have been received via email or available on a share. It will take a moment for this invitation to open.
  - Enter the password in the Windows Remote Assistance dialog box, and click OK.
  - If you enter an incorrect password, you will be notified immediately.
  - The user requesting help will see a dialog box appear asking whether they want to allow the connection.
  - The user should click Yes. At this point, you will be able to see everything on the user’s desktop, but you won’t be able to interact with the desktop.
  - Click the Request Control button at the top of the Windows Remote Assistance window.
  - The user will see a dialog box appear asking whether they want to allow the helper to share control of the desktop.
  - The user should click Yes.
  - Note that the user has complete control and can deny the request. However, since the user requested assistance and gave the password, they would click Yes.
  - The helper can now control the mouse on the remote computer along with the user.

Operating system security overview:- Windows Firewall

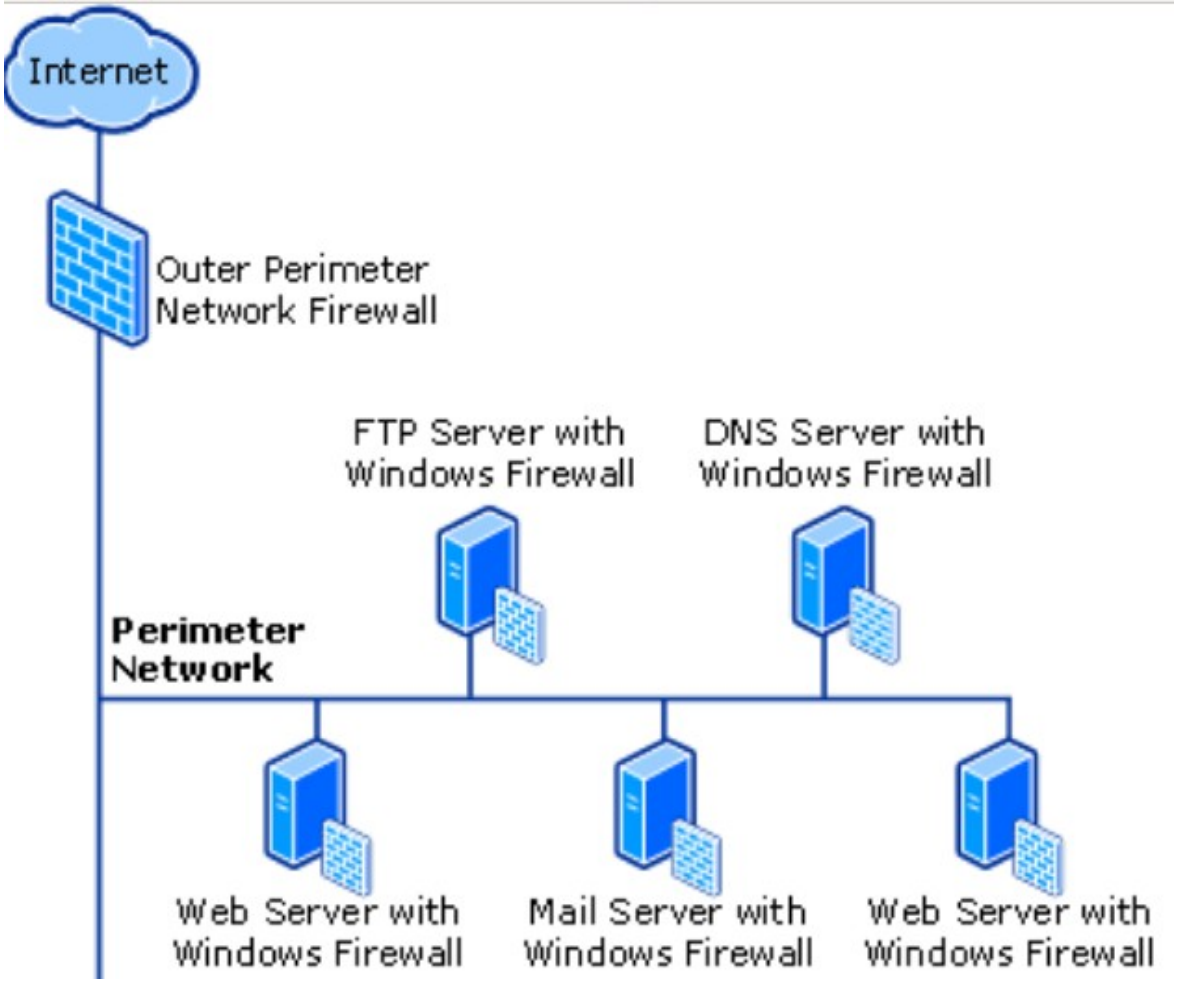
- Firewalls are packet filters which allows or denies each incoming and outgoing packet based on some rules defined by the administrator.
- The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall.
- Firewall is a single point through which all traffic happens.
- Limitations:
  - Cannot protect against attacks that bypass the firewall.
  - Firewall may not protect fully against threats from inside.
  - An improperly secured wireless LAN may be accessed from outside the organization.

Four Types of Firewalls

- Packet filtering firewall: Simply filters (forwards or denies) the packets from and to the network based on a set of rules.
- Stateful inspection firewall: Tightens the packet filtering by keeping records of each incoming and outgoing TCP connections.
- Application proxy firewall (application-level gateway): It acts as a proxy between the user and the remote host. But actual connection is between the user and the remote host. Ie, a single TCP connection between the two.
- Circuit-level proxy firewall (circuit-level gateway): It acts as a proxy between the user and the remote host. But the user is communicating with the proxy only, and the proxy is communicating with the remote host. There are two distinct TCP connections.

Windows Firewall inspects and filters all IP version 4 (IPv4) and IP version 6 (IPv6) network traffic.

- It is a stateful firewall inside the Windows Operating System, which means it tracks the state of each network connection and determines whether incoming traffic is allowed or blocked.
- Windows Firewall blocks incoming traffic unless it is in response to a request by the host or has been specifically allowed.
- Windows Firewall allows all outgoing traffic except some types of ICMP messages.
- You cannot use Windows Firewall as a perimeter firewall.



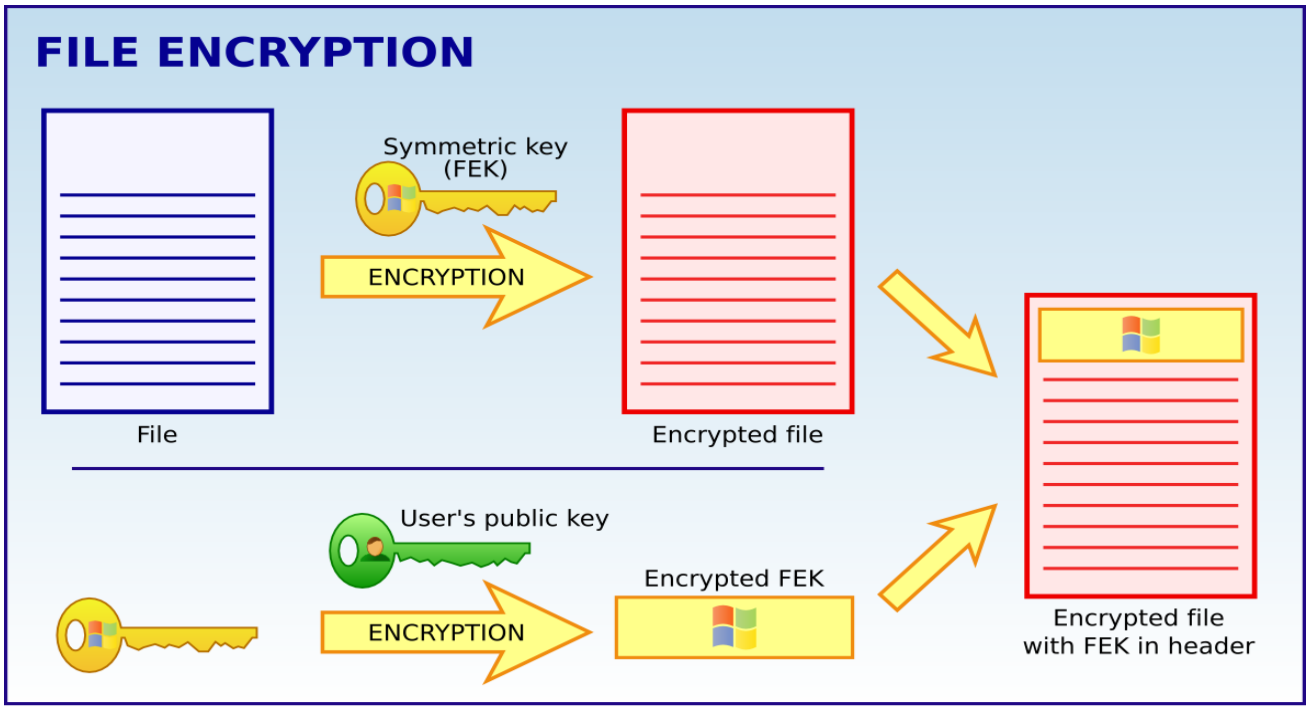
Encryption techniques

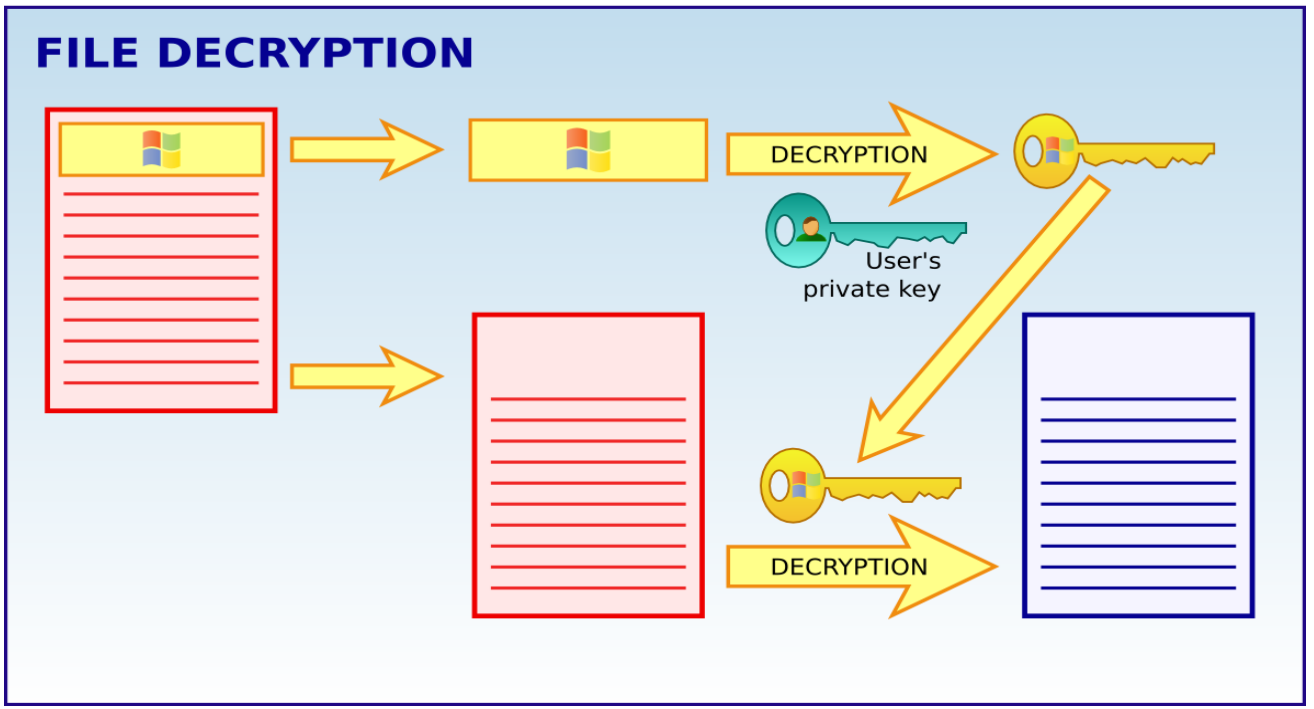
- The Encrypting File System (EFS) on Microsoft Windows is a feature of NTFS that provides filesystem-level encryption.
- The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer.
- By default, no files are encrypted, but encryption can be enabled by users on a per-file, per-directory, or per-drive basis.
- Some EFS settings can also be mandated via Group Policy in Windows domain environments.
- Operation:
  - Works using both symmetric (one key is used to encrypt the files) and asymmetric (two keys are used to protect the encryption key) encryption.
  - Encryption:

    Since symmetric encryption works easily even on large files, primary encryption is symmetric using system generated sytmmetric key (known as File Encryption Key, or FEK). This key is encrypted using the user's public key and stored along with the encrypted file.
  - Decryption:

    When the user unters his private key, it is used to decrypt the symmtric key; which is in turn used to decrypt the original file.

Encryption techniques...





Encryption techniques: Using BitLocker

- BitLocker is a full disk or drive encryption feature included with Windows Vista and later.
- It is designed to protect data by providing encryption for entire volumes.
- By default it uses the AES (Advanced Encryption Standard) encryption algorithm with a 128-bit or 256-bit key.
- BitLocker can be installed using “Add Roles and Features' in the server.
- There are three authentication mechanisms that can be used as building blocks to implement BitLocker encryption:

1) Transparent operation mode: The key is sealed in a Trusted Platform Module (TPM) chip and fixed in the machine. It releases the key to the specified OS components on booting.
2) User authentication mode: The user provides some authentication to the pre-boot environment in the form of a pre-boot PIN or password.
3) USB Key Mode: The user must insert a USB device (smart cards) that contains a startup key into the computer to be able to boot the protected OS. The CCID (chip card interface device) protocol in the smart card hides the private key using a cryptographic processor embedded in it.

IP Security

- Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services.
- IPSec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.
- IPSec policies can be assigned through Group Policy configuration of AD domains and OUs.
- Benefits of IP Security:
  - **Open industry standard:** IPSec provides an open industry-standard alternative to proprietary IP-based security technologies. Network managers benefit from the resulting interoperability.
  - **Transparency:** IPSec exists below the transport layer, making it transparent to applications and users, meaning there is no need to change network applications on a user's desktop when IPSec is implemented in the firewall or router.
  - **Authentication:** Strong authentication services prevent the acceptance of data through the use of falsely claimed identities.
  - **Confidentiality:** Confidentiality services prevent unauthorized access to sensitive data as it passes between communicating parties.
  - **Data origin authentication and integrity:** Data origin authentication and integrity is provided by a hashed message authentication code (HMAC) value, which is included in every packet.

IP Security...

- **Dynamic re-keying:** Dynamic re-keying during ongoing communications eliminates manual reconfiguration of secret keys and helps protect against secret key determination.
- **Secure links end to end:** IPSec provides secure links end-to-end for private network users within the same domain or across any trusted domain.
- **Centralized management:** Network administrators use IPSec policies to provide appropriate levels of security, based on user, work group, or other criteria. Centralized management reduces administrative overhead costs.
- **Flexibility:** The flexibility of IPSec allows policies to apply enterprise-wide or to a single workstation.

- Modes of operation

  IPSec can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

  - Transport mode: only the payload of the IP packet is usually encrypted or authenticated.
  - Tunnel mode: In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications, host-to-network communications and host-to-host communications.

System Backup

- A system backup is the process of backing up the operating system, its state, files and system-specific useful/essential data to another storage media so that if an error occurs to the main storage, they can be reloaded through a process called *restore*.
- Backup Types:

1) A normal backup copies all selected files and marks each as having been backed up. With normal backups, you need only the most recent copy of the backup file to restore all of the files.

2) An incremental backup backs up only those files created or changed since the last normal or incremental backup. It marks files as having been backed up. If you use a combination of normal and incremental backups, you need the last normal backup set as well as all the incremental backup sets to restore your data.

3) A differential backup copies files created or changed since the last normal or incremental backup. It does not mark files as having been backed up. If you are doing normal and differential backups, you must have the last normal and last differential backup sets to restore.

4) A copy backup copies all selected files but does not mark each file as having been backed up. Copying is useful to back up files between normal and incremental backups, because it does not affect other backup operations.

5) A daily backup copies all selected files that have been modified on the day that the daily backup is performed. The backed up files are not marked as having been backed up.

System Backup: Active Directory Backup

- **Windows Server Backup (WSB)** is a feature that provides backup and recovery options for Windows server environments.
- Administrators can use WSB to back up a full server, the system state, selected storage volumes or specific files or folders, as long as the data volume is less than 2 terabytes.
- the System State data includes Active Directory and all other system components and services on which Active Directory is dependent.
- WSB can be installed using Add Roles and Features in the Server Manager.
- The WSB utility lets create and manage backups, restore files and see the system's status.
- It gives the possibility to backup data from the server to a local disk (ideally a second disk attached to the server) or on a network share.
- Microsoft also allows to store backups in its clousd storage Microsoft Azure.
- The biggest difference between storing backups in a network shared folder versus using a local disk is that Windows Server Backup will store multiple versions of backups on a local disk but will store only the most recent version of a backup in a remote location.
- Local disk backups help to recover from multiple backups based on dates.
- The easiest and best method to backup is a **full-server backup**.
- It helps to recover even each file/folder, and the server OS itself.
- But needs lot of space and time.

System Backup: Active Directory Backup...

- When you use Windows Server Backup to back up the critical volumes on a domain controller, the backup includes all data that resides on the volumes that include the following:
  - The volume that hosts the boot files, which consist of the Bootmgr file and the Boot
  - The volume that hosts the Windows operating system and the registry
  - The volume that hosts the SYSVOL tree
  - The volume that hosts the Active Directory database (Ntds.dit)
  - The volume that hosts the Active Directory database log files
- Backup Modes
  - Manual backup: A member of the Administrators group or the or Backup Operators group can initiate a manual backup by using Server Backup each time that a backup is needed.
  - Scheduled backup: A member of the Administrators group can use the Windows Server Backup to schedule backups. The scheduled backups must be made on a local, physical drive that does not host any critical volumes.