## WINDOWS SERVERS OVERVIEW

Windows Server is available in 4 editions which include Foundation, Essentials, Standard and Datacenter, Azure Datacenter

| **Server Versions / Features** | **Released** | **Editions** | **Support** |
|---|---|---|---|
| Window Server 2022<br>High virtualization, Advanced multi-layer security | March 2022 | • Standard<br>• Datacenter<br>• Essentials<br>• Azure Datacenter | Next 10 to 15 yrs |
| Windows Server 2019<br>Windows admin center, shielded VM, Replica, Migration services, Improved windows defender | November 13, 2018 | • Windows Server 2019 Essentials<br>• Windows Server 2019 Standard<br>• Windows Server 2019 Datacenter | • Mainstream support until January 9, 2024<br>• Extended support until January 9, 2029 |
| Windows Server 2016<br>Network controller to manage switches and subnets | October 12, 2016 | • Windows Server 2016 Essentials<br>• Windows Server 2016 Standard<br>• Windows Server 2016 Datacenter | • Mainstream support ends on January 11, 2022<br>• Extended support ends on January 12, 2027 |
| Windows Server 2012<br>Private Cloud, powershell for admins storage tiers to add on to the storage and boost performance | September 4, 2012 | • Windows Server 2012 R2 Foundation<br>• Windows Server 2012 R2 Essentials<br>• Windows Server 2012 R2 Standard | • Mainstream support ended on October 9, 2018<br>• Extended support ends on October 10, 2023 |

| | | | |
|---|---|---|---|
| Windows Server 2012 R2 | October 17, 2013 | • Windows Server 2012 R2 Datacenter | |
| Windows Server 2008<br><br><br>Windows Server 2008<br>Hyper v, event viewer, server manager<br>Enhanced group policy, Remote Desktop | October 22, 2009<br><br>February 27, 2008 | • Windows Server 2008 R2 Foundation<br>• Windows Server 2008 R2 Standard<br>• Windows Server 2008 R2 Enterprise<br>• Windows Server 2008 R2 Datacenter<br>• Windows Server 2008 R2 for Itanium-based Systems<br>• Windows Web Server 2008 R2<br>• Windows Storage Server 2008 R2<br>• Windows HPC Server 2008 R2<br>• Windows Small Business Server 2011<br>• Windows MultiPoint Server 2011<br>• Windows Home Server 2011<br>• Windows MultiPoint Server 2010 | • Mainstream support ended on January 13, 2015<br>• Extended support ended on January 14, 2020 |

| | | | |
|---|---|---|---|
| Windows Server 2003 R2<br><br>NAT, encryption, built in firewall<br><br>Windows Server 2003 | December 6, 2005<br><br>April 24, 2003 | • Windows Small Business Server 2003<br>• Windows Server 2003 Web Edition<br>• Windows Server 2003 Standard Edition<br>• Windows Server 2003 Enterprise Edition<br>• Windows Server 2003 Datacenter Edition<br>• Windows Storage Server | • Mainstream support ended on July 13, 2010<br>• Extended support ended on July 14, 2015 |
| Windows 2000<br>Active directory services, Management Console, Dynamic disk volumes, NTFS file systems | February 17, 2000 | • Windows 2000 Server<br>• Windows 2000 Advanced Server<br>• Windows 2000 Datacenter Server | • Mainstream support ended on June 30, 2005<br>• Extended support ended on July 13, 2010 |
| Windows NT 4.0<br>Workstations and server workgroups, IIS, DNS | July 29, 1996 | • Windows NT 4.0 Server<br>• Windows NT 4.0 Server Enterprise<br>• Windows NT 4.0 Terminal Server Edition | • Mainstream support ended on December 31, 2002<br>• Extended support ended on December 31, 2004 |

| | | | |
|---|---|---|---|
| Windows NT 3.51 | May 29, 1995 | • Windows NT 3.51 Server | • Unsupported as of December 31, 2001 |
| Windows NT 3.5 | September 20, 1994 | • Windows NT 3.5 Server | • Unsupported as of December 31, 2001 |
| Windows NT 3.1 | July 27, 1993 | • Windows NT 3.1 | • Unsupported as of December 31, 2000 |

## SYSTEM REQUIREMENTS

Although most of the servers nowadays probably have the necessary requirements for Windows Servers, it will certainly be useful to know them in case you want to upgrade from an older system. The basic requirements are:

- CPU socket minimum 2.4 GHz (64-bit processor) or faster for single core and Microsoft recommends is 3.1 GHz (64-bit processor) or faster multi-core.
- RAM memory minimum is 8 GB, but Microsoft recommends 8GB.
- 500 GB hard disk with a 100 GB system partition space in your hard disk

One important thing to note here is that the installation process itself will verify your computer hardware and let you know if it qualifies for a Windows Server 2012 installation. If not, then you will need to upgrade your hardware.

# WINDOWS SERVER

## INTRODUCTION

### The Windows Server Family

Server started with the Windows Server NT was the first 32bit (*A 32-bit microprocessor can process data and memory addresses that are represented by 32 bits*.) operating system, 2000, 2003, 2008

As new releases are developed they come with security, more reliability, more availability, and easier to administer than any previous version of Windows.

## WINDOWS SERVER EDITIONS

Windows Servers are mostly available in 64-bit. But the most important distinctions are those among the following four product editions:-

1. STANDARD EDITION

This is a robust, multipurpose server capable of providing directory, file, and print, applications, multimedia, and Web services for small to medium-sized businesses. Its comprehensive feature set is expanded e.g. SQL Server Database Engine **(MSDE),** a version of SQL Server that supports five concurrent connections to databases up to 2 GB in size; a free, out-of-the-box Post Office Protocol version 3 (POP3) service which, combined with the included Simple Mail Transfer Protocol (SMTP) service, allows a server to function as a small, stand-alone mail server; and Network Load Balancing (NLB). This edition supports up to 4 GB of RAM and four-way SMP.

2. ENTERPRISE EDITION

The Enterprise Edition is designed to be a powerful server platform for medium- to large-sized businesses. Its enterprise-class features include support for eight processors, 32 GB of RAM, eight-node clustering (*A cluster is a group of computers, called nodes that* function as a single computer/system to provide high availability and high fault

tolerance for applications or services. Windows Servers can participate in a cluster configuration through the use of Cluster Services. If one member of the cluster (the node) is unavailable, the other computers carry the load so that applications or services are always (with a small interruption) available.) (Including clustering based on a Storage Area Network (SAN) and geographically dispersed clustering) and availability for 64-bit Intel Itanium-based computers, on which scalability increases to 64 GB of RAM and 8-way SMP.

**Distinguishing features of the Enterprise Edition**

- Hot Add Memory, so that you can add memory to supported hardware systems without downtime or reboot
- Windows System Resource Manager (WSRM), which supports the allocation of CPU and memory resources on a per-application basis

### 3. DATACENTER EDITION

The Datacenter Edition, which is available only as an OEM (*original equipment manufacturer*) version as part of a high-end server hardware package, provides almost unfathomable scalability, with support on 32-bit platforms for 32-way SMP with 64 GB of RAM and on 64-bit platforms for 64-way SMP with 512 GB of RAM.

## UNDERSTANDING NETWORK INFRASTRUCTURES

A *network infrastructure* is a set of physical and logical components that provide the basis for connectivity, security, routing, management, access, and other integral features on a network.

Most frequently, a network infrastructure is both *inherited* and *designed*. If a network connects to the Internet, certain aspects of the network, such as the Transmission

Control Protocol/Internet Protocol (**TCP/IP**) protocol suite, are inherited from the Internet. Other network aspects, such as the physical layout of basic network elements can be designed.

## TYPES OF INFRASTRUCTURES

### *a) Physical Infrastructure*

A network's *physical infrastructure* is its *topology*—the physical design of the network—along with hardware components such as cabling, routers, switches, bridges, hubs, servers, and hosts. The physical infrastructure also includes technologies such as Ethernet, 802.11b wireless, Public Switched Telephone Network (**PSTN**), and Asynchronous Transfer Mode (**ATM**), all of which define methods of communication over certain types of physical connections.

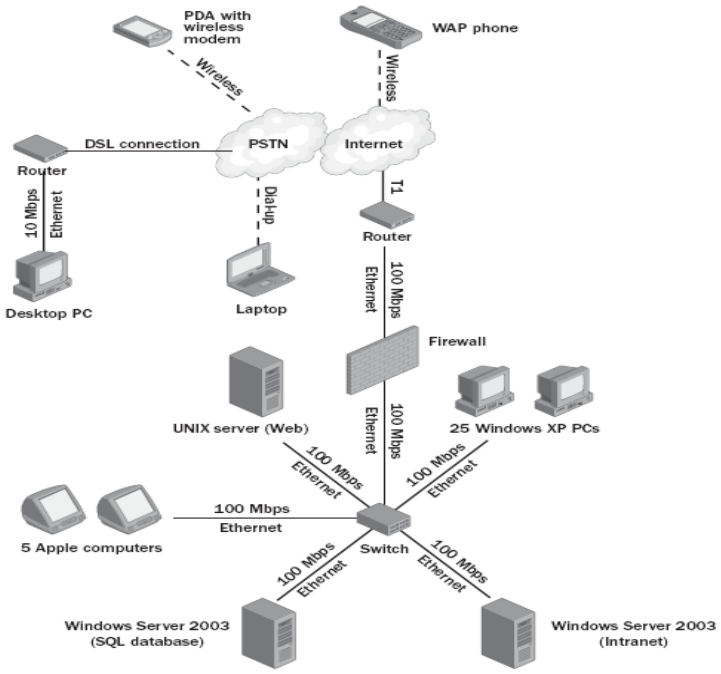



**Figure 1-1** Physical infrastructure of a network

### *b) Logical Infrastructure*

The *logical infrastructure* of a network is composed of the many software elements that connect, manage, and secure hosts on the network. It allows for communication between computers over the pathways that are described in the physical topology. Example elements of the logical infrastructure include network components such as Domain Name System (DNS), network protocols such as TCP/IP etc.

Once a network has been designed, the maintenance, administration, and management of its logical infrastructure require many aspects of the network's technologies. E.g. create various types of network connections; how to install and configure network protocols required for various network needs; how to configure manual and automatic addressing methods appropriate to network needs; how to configure name resolution methods; and how to troubleshoot network problems related to connectivity, addressing, access, security, and name resolution, virtual private networks (**VPNs**).

(*A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's LAN.*

*A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and* ***tunneling protocols*** *such as the* ***Layer Two Tunneling Protocol (L2TP)****. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted.*
*An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.)*

## LOGICAL ELEMENTS OF WINDOWS SERVER

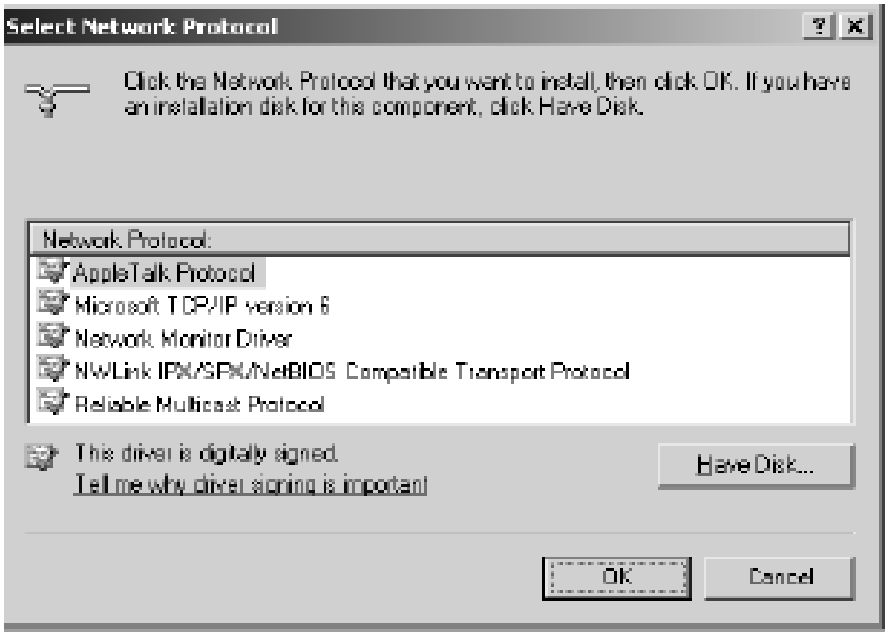
### a) Network Connections

In Microsoft Windows, *network connections* are logical interfaces between software (such as protocols) and hardware (such as modems or network adapters). Network connections can be seen in the Network Connections window as shown in the figure. Connections are prioritized and are normally configured with various types of protocols, services, and client software


### b) Network Protocols

These are network languages used for computer-to-computer communication. E.g. Windows networks, UNIX networks, and the Internet all rely on the TCP/IP network protocol for basic communication. In Windows, connections can communicate with foreign hosts only by using network protocols that are installed on the local computer and bound to that connection. TCP/IP is installed and bound by default to every connection. *TCP/IP is actually a group of protocols referred to as a stack or suite. This protocol*

*stack includes Address Resolution Protocol (ARP), Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and many others.*




### c) Network Services

These are programs that provide features, such as quality of service, to hosts or protocols on a network.

### d) Network Clients

In Windows, *network clients* are programs that allow a computer to connect to a network operating system. For example, by installing Client Service for NetWare and binding the service to a particular connection, you can connect to Net- Ware networks.

### e) Addressing

*Addressing* is the practice of configuring devices with IP addresses in order to communicate with other devices on a network. An IP address is a logical network address that identifies a particular host and it must be properly configured and unique.

IP version 4 provides a method for computers with 4-byte addresses to communicate with each other. IP Addresses can be configured manually, distributed automatically through the use of a DHCP server, or self-configured.

### f) Name Resolution

Most networks use a naming system so that people can refer to computers by name instead of by address. *Name resolution* is the process of translating a computer name into an address, and vice versa. Since Windows can use two different naming systems, NetBIOS and DNS, Windows networks support two name resolution systems.

DNS is the native naming system of the Internet and all Windows operating systems released since Microsoft Windows 2000. To resolve NetBIOS names, Microsoft networks can send broadcast queries to all systems on the same network segment or send requests to a WINS server. To resolve DNS (host) names, Microsoft networks rely on the DNS protocol and DNS servers. To function properly, both of these name resolution services must be configured.

### g) Network Computer Groups

In Windows, computers can be grouped into workgroups or domains.

- A ***workgroup*** is a simple grouping of resources intended to help users find such resources as printers and shared folders. By default, computers in Windows workgroups use the NetBIOS naming system to name computers and resolve those names. NetBIOS is used with associated protocols, such as Common Internet File System (CIFS)—an extension of the Server Message Block (SMB) protocol—to provide file sharing, security for network shares, and network browsing features. There is no centralized security or management features are available.

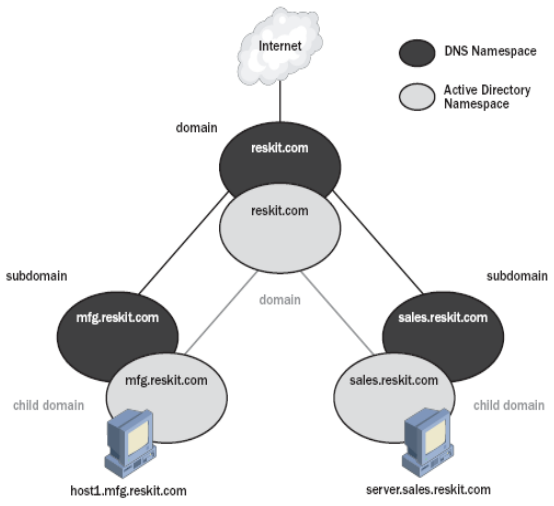
- A ***domain*** is a collection of computers, defined by a network administrator, that share a common directory, security policies, and relationships with other domains. Security and directory information are stored in domain controllers within each domain.

### h) Active Directory

*Active Directory* is a distributed database and directory service that is replicated among all domain controllers on the network. The Active Directory database stores information about network objects including domains, computers, users, and other objects. The distributed nature of Active Directory gives network users access to permitted resources anywhere on the network by using a single logon process. It also provides a single point of administration for all network objects.

The term *domains* is used to refer both to groupings of computers in Active Directory and to hierarchical name suffixes such as microsoft.com in DNS. Remember that Active Directory domains and DNS domains are separate entities governed by separate systems.

To simplify administration, Active Directory domains and their member computers are normally assigned names that match DNS names. In this way, the Active Directory namespace and the DNS namespace overlap.



### i) Remote Access

*Remote access* connections must be configured for users who connect to a Windows network from a nonlocal site. The two basic methods for remote access include direct dial-up to a network computer and virtual private networks. For dial-up access, you must not only configure a server to answer incoming calls, but you must also configure authentication, access permissions, and encryption requirements. VPNs enable private connections to cross a public network such as the Internet. These network connections require a different set of configuration procedures for authentication, encryption, and security.

### j) Network Address Translation

*Network Address Translation* (NAT) is a method of allowing computers internal to your network that have been given nonpublic addresses to communicate with computers on the Internet. When you configure NAT to be used with your network infrastructure, this setup affects the addressing scheme of your network. *Internet Connection Sharing* (ICS) is a simple implementation of NAT included with recent Windows operating systems.

### i) Certificate Infrastructure

*Certificates* are used for public key cryptography, which is an important security element in Windows Server networks. Certificates and public key cryptography are used in many Windows features, such as the Secure Sockets Layer (SSL), the Internet Protocol Security (IPSec) protocol (which encrypts IP communications), smart cards, and the Encrypting File System (EFS, which secures files on a network). The certificate infrastructure supported in Windows Server networks integrates with the *Public Key Infrastructure* (PKI) system: a system of digital certificates, certification authorities, and other registration authorities that authenticate each party involved in an electronic transaction.

## WINDOWS SERVER ROLES

Windows Server can be configured to perform the following roles:

**Domain controller:** used to manage domains and domain objects; provides user authentication through Active Directory.

**File server:** provides access to files stored on the server.

**Print server:** provides network printing functionality.

**DHCP server:** allocates IP addresses and provides configuration information to clients.

**DNS server:** resolves IP addresses to domain names.

**Mail server:** provides incoming (POP3) and outgoing (SMTP) e-mail services.

**Application server:** makes distributed applications and Web applications available to clients.

**Terminal server:** allows clients to access applications running on the server.

**Remote access/VPN server:** provides remote access to machines through dial-up connections and virtual private networks (VPNs).

**Streaming media server:** provides Windows Media Services so that clients can access streaming audio and video.

## 1. Domain Controllers (Authentication Servers)

Domain controllers are required to manage domains and domain-based objects. One important aspect of this is user authentication and access control. In order to carry out these functions, the domain controller must have information about users and other objects in the domain.

### *Active Directory*

Active Directory stores information about network resources and makes these resources accessible to users, computers and applications by uniquely identifying them on the network. It provides mechanisms for naming, describing, locating, accessing, managing and securing network resources.

Active Directory also allows for the central management of the Windows Server network, and for the delegation of administrative control over Active Directory objects, such as user data, printers, servers, databases, groups, computers and security principals and security policies that are stored in the directory. In other words, the Active Directory service provides the structure and functions for organizing, managing, and controlling network resources.

## 2. File and Print Servers

When a Windows Server computer is configured as a file server or print server, additional functions become available that makes using and managing the server more effective.

Print servers are used provide access to printers across the network. They offer an added level of manageability for network printing and allow an administrator to control when print devices can be used by scheduling the availability of printers, setting priority for print jobs and configuring printer properties. An administrator can also view, pause, resume, and/or delete print jobs and manage printers remotely and by using *Windows Management Instrumentation (WMI),* which allows an administrator to manage components like print servers and print devices from the command line.

File servers are used to store data in a central location, so they must be kept secure to ensure that only those who are authorized are able to use the files.

The volumes on a file server should be formatted with *NTFS* to allow file and folder permissions to be set and the Encrypting File System (EFS) should be used to guard against unauthorized users and malicious programs. Although encryption and decryption can be complex, EFS file encryption is completely transparent to the user. However, you cannot encrypt system files and you cannot share encrypted. Encrypted files cannot be compressed and compressed files will be decompressed when you encrypt them.

File servers allow users to store their files remotely, rather than on their local hard disks, and share them with other users. When a file is saved to a file server, clients who have access to the relevant directory can access it remotely. File servers are also important when multiple employees use network-accessible applications and data may need to be saved to a shared database, spreadsheet or other type of file.

### 3. DHCP SERVERS

A *Dynamic Host Configuration Protocol* (DHC'P) Server automatically issues IP addresses to clients on TCP/IP networks. Each IP address uniquely identifies a client and allows it to send and receive packets of data. Each packet contains the IP address of the sender and the receiver, so no two clients can have the same IP address at the same time.

DHCP assigns IP addresses dynamically. The client contacts the DHCP server requesting an IP address and the DHCP server responds by issuing an IP address from a pool of available addresses and as other IP configuration details, such as WINS or DNS server information, needed by the client.

DHCP servers do not require authentication when providing a lease, so any client that contacts the DHCP server can obtain a lease and connect to the network. It is therefore important to restrict physical and wireless access to your network to prevent unauthorized clients from connecting to your network and obtaining a DHCP lease. Auditing should be enabled on the DHCP server and the logs reviewed regularly for possible problems.

Issuing out bogus DHCP leases that do not expire can be a very effective Denial of Service (DoS) technique, so it is important to monitor network traffic for DHCP server traffic that does not come from authorized DHCP servers.

You need to be a member of the Administrators group or the DHCP Administrators group to administer DHCP servers remotely using the DHCP console, so restricting membership in these groups limits the number of people who can authorize a DHCP server.

## 4. Domain Name Resolution

Windows Servers makes use of user-friendly domain names to represent the IP address of a host or a client. This implies the use of some kind of name resolution so that a computer can identify the IP address that a user-friendly name corresponds to. Windows Server uses *Windows Internet Naming Service* (WINS) and *Domain Name Service* (DNS) to provide name resolution.

WINS resolves IP addresses to NetBIOS names and vice versa. NetBIOS names provide backwards compatibility for pre-Windows 2000 clients and servers and allow users of those previous versions of windows

*The Domain Name Service* (DNS) is a common method of name resolution that is widely used on TCP/IP networks. In Windows Servers, Active Directory is integrated with DNS and

uses DNS servers to allow users, computers, applications, and other elements of the network to find domain controllers and other resources on the network.

DNS is a hierarchical, distributed database that maps between user-friendly domain names (like www.google.com) and IP addresses. Every time a user enters a domain name into a browser or other application, it is forwarded to a DNS server, which *looks up* the IP address corresponding to that domain. This IP address is sent back to the client, which uses it to locate and communicate with the corresponding computer.

### 5. WEB SERVERS

Web servers allow organizations to host their own Web sites on the Internet or a local intranet. Users can benefit by accessing information, downloading files and using Web-based applications. Internet Information Services (IIS), bundled with Windows Server, is required for configuring a Web Server, and allows users to access information using several protocols that form part of the TCP/IP protocol suite.

- *Hypertext Transfer Protocol (HTTP):* used by the World Wide Web Publishing service in IIS. It allows users to access Web pages using a Web browser or other Web-enabled applications. HTTP supports the Hypertext Markup Language (HTML), Active Server Pages (ASP) and Extensible Markup Language (XML).
- *File Transfer Protocol (FTP):* used for transferring files between clients and servers. Clients can use this service to copy files to and from FTP sites using a Web browser or an FTP client.
- *Network News Transfer Protocol (NNTP):* used for newsgroups (discussion groups). The NNTP service in IIS allows users to browse stored messages, respond to existing messages, and post new ones using a newsreader program.
- *Simple Mail Transfer Protocol (SMTP):* used to provide e-mail capabilities. The SMTP service included in IIS provides limited e-mail services.

### 6. HYPER-V

The *Hyper-V role* in Windows Server lets you create a virtualized computing environment where you can create and manage virtual machines. You can run multiple operating systems on one physical computer and isolate the operating systems from each other.

With this technology, you can improve the efficiency of your computing resources and free up your hardware resources. Provides the services that you can use to create and manage *virtual machines* (VMs) and their resources.

### 7. TERMINAL SERVICES

Enables users to access Windows-based programs that are installed on a terminal server or to access the Windows desktop from any computing device that supports the *Remote Desktop Protocol (RDP)* protocol

Users can connect to a terminal server to run programs and to use network resources on that server. Server 2008 has technologies that allow the *RDP* traffic necessary for communication with a terminal server from a client to be encapsulated in HTTPS packets, which means all communication is via port *443* so no special holes are required in the firewall for access to terminal servers within an organization from the Internet.

### 8. EMAIL CLIENTS AND SERVERS (E-MAIL SERVICE)

Email is one of the most popular client/server applications on the Internet. Email servers run server software that enables them to interact with clients and with other email servers over the network.

Each mail server receives and stores mail for users who have mailboxes configured on the mail server. Each user with a mailbox must then use an email client to access the mail server and read these messages.

Mail servers are also used to send mail addressed to local mailboxes or mailboxes located on other email servers.

Mailboxes are identified by the format: user@company.domain.

Various application protocols used in processing email include SMTP, POP3, and IMAP4.

## REQUIREMENTS FOR PRIVILEGED ACCESS MANAGEMENT

- Microsoft Identity Manager
- Active Directory forest functional level of Windows Server
- Stage 1 of the Security Privileged Access roadmap includes these components:

### *1. Separate Admin account for admin tasks*

To help separate internet risks (phishing attacks) from administrative privileges, create a dedicated account for all personnel with administrative privileges.

### *2. Privileged Access Workstations (PAWs) -Active Directory admins*

To help separate internet risks from domain administrative privileges, create dedicated privileged access workstations (PAWs) for personnel with AD administrative privileges.

### *3. Unique Local Admin Passwords for Servers and Workstations*

To mitigate the risk of an adversary stealing a local administrator account password hash from the local SAM database and abusing it to attack other computers, you should use the *Local Administrator Password Solution* (LAPS) tool to configure unique random passwords on each workstation and server and register those passwords in Active Directory.

### *4. Roaming Profiles*

To enable Users access their profiles from any workstation