6.1. Introductions
6.2. Benefits and drawbacks of intranets
6.3. Protocols, Structure and Scope of Networks
6.4. Intranets Resource Assessments: Network Infrastructure, Clients and Server Resources
6.5. Intranet Implementation Guidelines
6.6. Content Design, Development, Publishing and Management
6.7. Intranet Design with Open Source Tools: DRUPAL, JUMLA
6.8. Tunneling Protocols: VPN

6.1. Introductions

The Intranet is a network based on TCP/IP protocols belonging to an organization, accessible only by the organization's members, employees, or others with authorization. *See in Chapter-1.*

6.2. Benefits and drawbacks of intranets

Advantages of Intranets

Implementation benefits	▪ Fast, easy, low-cost to implement ▪ Based on open standards ▪ Connectivity with other systems ▪ Many tools available ▪ Scalable
Usability benefits	▪ Easy to learn and use ▪ Multimedia ▪ Hypertext links ▪ Single interface to information resources and services
Organizational benefits	▪ Access to internal and external information ▪ Improves communication ▪ Increases collaboration and coordination ▪ Supports links with customers and partners ▪ Can capture and share knowledge

- Intranets offering *workforce productivity* which can help user to find and observe *information very fast*. User may also use applications according to their roles and tasks. Through web browser a user can get access to entire contents of any website from anywhere or any time. Intranet also increase the ability of employee's by performing their job confidently very fast, and accurately.
- Intranet permits business companies to *share out information* to employees according to their need or requirements. Employees may also link to appropriate data at their expediency.
- The best advantage offered by intranet is *communications within an organization* or business company, landscape or portrait. Intranets are helpful to converse planned initiative that has an international reach all through the organization. The well known examples of transportation are chat, email, and blogs. A actual world example of Intranet is Nestle had a number of food processing plants.
- The most significant advantage of Intranet is *Web publishing* which permits burdensome corporate knowledge to be continued and effortlessly access all through the company using Web technologies and hypermedia. The familiar examples of web publishing consist of *training, news feed, company polices, documents, and employee manual*. Each unit can bring up to date the online copy of a document and intranet always provides the most recent version to employees.
- Intranet offering business operations and administration solutions because it also being used as a *platform of mounting and organizing applications* across the internet world.
- Another advantage of Intranet is *time saving* because there is no need to maintain physical documents such as procedure manual, requisition forms, and internet phone list.
- Now intranet facilitates their user to *view and gets information and data* via web browser. Intranet also save the money of any organization on printing, publishing and overall maintenance.
- Through Intranet common corporate culture every user can view the *similar information.*
- Intranet *offer improve teamwork* through which teamwork is enabled and all certified users can get access to information.
- Intranet providing *cross platform capability* for UNIX, Mac, Windows.
- Intranet offering their user to write applications on their browser without *cross-browser compatibility issues.*
- Intranet is a Web-based tool that permits users to produce a customized site according their requirements. You can pull all Internet actions and most wanted contented into a single page which make easier to access.

Disadvantages of Intranet

- Management does *need to stop control of specific information*; this problem can be minimized but with appropriate prudence.

- *Security issue:* Intranet gathered everything in one location which is really good but if it is not prearranged then you will spoil everything.
- *The cost of intranet is very high* but has lots of advantages after implementing.

6.3. Protocols, Structure and Scope of Networks

A protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities.

An intranet uses the same ideas and advancements as the World Wide Web and Internet. This incorporates web programs and servers running on the web convention suite and utilizing Internet conventions, for example, FTP, TCP/IP, Simple Mail Transfer Protocol (SMTP) etcetera. HTTP(s),SMTP(s) ,IMAP(s) ,POP3(s) ,DHCP ,DNS ,FTP ,SSH ,VOIP ,Active Directories or LDAP ,VPN

6.4. Intranets Resource Assessments: Network Infrastructure, Clients and Server Resources

Intranet Network Infrastructure:

A system foundation is an interconnected gathering of PC frameworks connected by the different parts of media communications engineering. In particular, this foundation mentions to the association of its different parts and their arrangement — from individual organized PCs to switches, links, remote access focuses, switches, spines, system conventions, and system access techniques. Bases can be either open or shut, for example, the open design of the Internet or the shut engineering of a private intranet. They can work over wired or remote system associations, or a mix of both.

The easiest type of system framework commonly comprises of one or more PCs, a system or Internet association, and a center point to both connections the PCs to the system association and attach the different frameworks to each other. The center point just connections the PCs, yet does not restrain information stream to or from any one framework. To control or farthest point access amongst frameworks and direct data stream, a switch replaces the center point to make system conventions that characterize how the frameworks speak with each other. To permit the system made by these frameworks to impart to others, by means of the system association, requires a switch, which connects the systems and essentially gives a typical dialect to information trade, as indicated by the tenets of every system.

Why Is the Network Infrastructure Important to Your Intranet?

An intranet is comprised of two sections: the applications (programming/conventions) and the system framework on which the applications run. Applications—the obvious part of an intranet — give the usefulness to enhance efficiency and lower costs. A wide range of Internet/intranet applications is accessible from numerous merchants. The system base incorporates the equipment—system interface cards (NICs), center points, switches, switches, and servers—over which the applications run. All system equipment is not the same, and an intranet is just as usable, solid, and savvy as the equipment on which it runs. Pivotal contemplations in picking proper equipment include:

- Bandwidth accessibility
- Reliability
- Value, as far as both starting expense and convenience and administration
- Scalability, to guarantee that present and future needs can be met

So as a piece of system framework, experience the above-highlighted parts. I think you have contemplated those in information correspondence also.

6.5. Intranet Implementation Guidelines

At the point when arranging an intranet, there are various inquiries to be considered. These inquiries will set the tone for how you develop your intranet, help you set up rules.

- What is your business case for building the intranet?
- Who can distribute to the intranet?
- What sorts of substance can be distributed?

- In order to develop a well structured and organized intranet that would fulfill all requirements, one would have to follow the right intranet development guidelines.
- Before starting developing intranet, one need to do extensive research and an in-depth needs analysis to find out what exactly your requirements are and what you want to achieve.
- The intranet development guidelines will help and guide during the different stages of the development process.
- The purpose and goals of the intranet
- Persons or departments responsible for implementation and management
- Functional plans, information architecture, page layouts, design
- Implementation schedules and phase-out of existing systems
- Defining and implementing security of the intranet
- How to ensure it is within legal boundaries and other constraints
- Level of interactivity (e.g. wikis, on-line forms) desired.
- Is the input of new data and updating of existing data to be centrally controlled or devolved

Actual Intranet Implementation Includes

- Securing senior management support and funding.
- Business requirements analysis.
- Identify users' information needs.
- Installation of web server and user access network.
- Installing required user applications on computers.
- Creation of document framework for the content to be hosted.
- User involvement in testing and promoting use of intranet.
- Ongoing measurement and evaluation, including through benchmarking against other intranets

6.6. Content Design, Development, Publishing and Management

Intranet Site Development

- An Intranet is a private network that uses common web technology for use within and enterprise or organization.
- Access to the network is restricted.
- Intranets may serve anything from small workgroups sharing the same office space to entire corporation with locations around globe.
- Intranet applications are typically used in "Business to Employee" (B2E) context, which means they are used to communicate with employees and share information within the organization
- A content management system is software that keeps track of every piece of content on Web site, much like local public library keeps track of books and stores them.
- Content can be simple text, photos, music, video, documents, or just about anything you can think of.
- A major advantage of using a CMS is that it requires almost no technical skill or knowledge to manage. Since the CMS manages all content, one don't have to.

Substance is a substance, and data on the webpage should be applicable to the webpage and should focus on the range of people in general that the site is worried with.

Content Management:

Content administration, or CM, is the arrangement of procedures and innovations that backing the gathering, overseeing, and distributed of data in any structure or medium. As of late this data is regularly mentioned to as substance or, to be exact, advanced substance. Computerized substance may appear as content, (for example, electronic records), mixed media documents, (for example, sound or video documents), or some other record sort that takes after a substance lifecycle requiring administration. A basic part of substance administration is the capacity to oversee forms of substance as it advances

Content administration is an inalienably community process. It frequently covers of the accompanying fundamental parts and obligations:

- Creator - in charge of making and altering content.
- Editor - in charge of tuning the substance message and the style of conveyance, including interpretation and confinement.
- Publisher - in charge of discharging the substance for use.
- Administrator - in charge of overseeing access authorizations to organizers and records, normally expert by appointing access rights to client gatherings or parts. Administrators may likewise help and bolster clients in different ways.
- Consumer, viewer or visitor the individual who peruses or generally takes in substance after it is distributed or shared.

A substance administration framework is an arrangement of computerized procedures that may bolster the accompanying components:

- Import and formation of reports and media material.
- Identification of every single key client and their parts.
- The capacity to dole out parts and obligations to various examples of substance classifications or sorts.
- Definition of work process assignments frequently combined with informing so that substance directors are alarmed to changes in substance.
- The capacity to track and deal with various adaptations of a solitary example of substance.
- The capacity to distribute the substance to an archive to bolster access to the substance. Progressively, the vault is an inborn part of the framework and fuses venture inquiry and recovery.

6.7. Intranet Design with Open Source Tools: DRUPAL, JUMLA

***Drupal (Open Source CMS)**: https://www.drupal.org/ , https://en.wikipedia.org/wiki/Drupal

Drupal content administration framework or Drupal CMS is an open source particular structure and Content Management System written in PHP that can be utilized to deal with your site or blog from an online interface. Drupal is utilized as a "back end" framework for a wide range of sorts of sites; going from a little individual site to huge corporate locales. It permits an individual or a group of clients to effortlessly distribute, oversee and compose a wide assortment of substance on a site.

Joomla - The CMS Trusted By Millions for their Websites: https://www.joomla.org/ , https://en.wikipedia.org/wiki/Joomla

Joomla CMS is a web application that makes it simple for any individual to assemble a site. A site made with custom Joomla plan permits the client to take control of their site. The excellence of Joomla is that the fashioners can influence the current system and UI to convey applications to the end clients in a recognizable, effective environment. This procedure spares time and also chops the financial backing down.

Comparison between JOOMLA and Drupal :-

	JOOMLA	DRUPAL
Popularity	63 million downloads	15 million downloads
Free Themes	1K+	2K+
Free Plugins	7K+	34K+
Top sites using this platform	Harvard University, Linux, THE HILL	The white house, WB
Ease of moderation	2 star	3 star
Updates frequency	36 days	51 days
Best used for	e-commerce, social site networking	One size fits all

6.8. Tunneling Protocols: VPN

A **tunneling protocol** *allows a network user to access or provide a network service that the underlying network does not support or provide directly.* Importance of tunneling protocol are :-

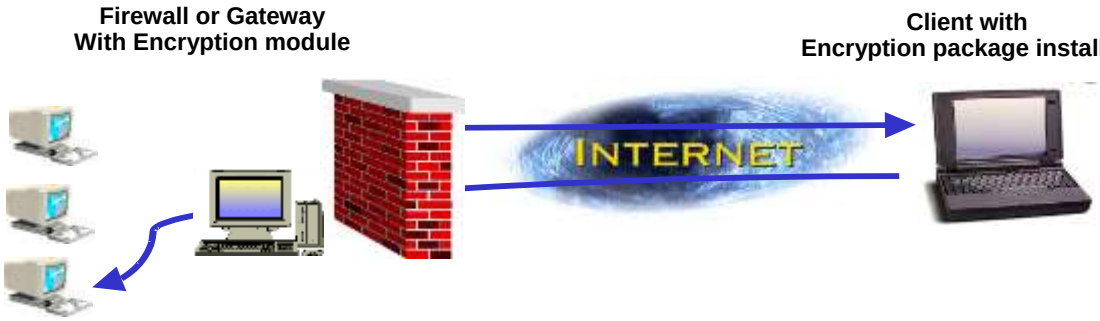
- to *allow a foreign protocol to run over a network that does not support that particular protocol; for example*, running IPv6 over IPv4.
- use is to provide services that are *impractical or unsafe to be offered using only the underlying network services; for example,* providing a corporate network address to a remote user whose physical network address is not part of the corporate network. Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, a third use is to hide the nature of the traffic that is run through the tunnels.

The *tunneling protocol works by using the data portion of a packet (the payload) to carry the packets that actually provide the service*. Tunneling uses a layered protocol model such as those of the OSI or TCP/IP protocol suite, but usually violates the layering when using the payload to carry a service not normally provided by the network. Typically, the delivery protocol operates at an equal or higher level in the layered model than the payload protocol.

Types of VPN

1. **Firewall-to-Firewall VPN**
   - Data is encrypted when it leaves Firewall #1 and crosses the Internet
   - The data is authenticated and decrypted when it reaches Firewall #2.

2. **Client-to-Firewall VPN**



Different types of VPN tunneling or VPN Modes:

- ***Voluntary VPN tunneling:*** the *VPN client manages connection setup*. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs). Then, the VPN client application creates the tunnel to a VPN server over this live connection.
- ***Compulsory VPN Tunneling:*** the *carrier network provider manages VPN connection setup*. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. From the client point of view, VPN connections are set up in just one step compared to the two-step procedure required for voluntary tunnels.

- Host to Gateway/ remote-access VPNs
  - Remote access VPN allows a user to connect to a private network and access its services and resources remotely. The connection between the user and the private network happens through the Internet and the connection is secure and private.
  - Remote Access VPN is useful for business users as well as home users.
  - A corporate employee, while traveling, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network.
  - Home users, or private users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users conscious of Internet security also use VPN services to enhance their Internet security and privacy.

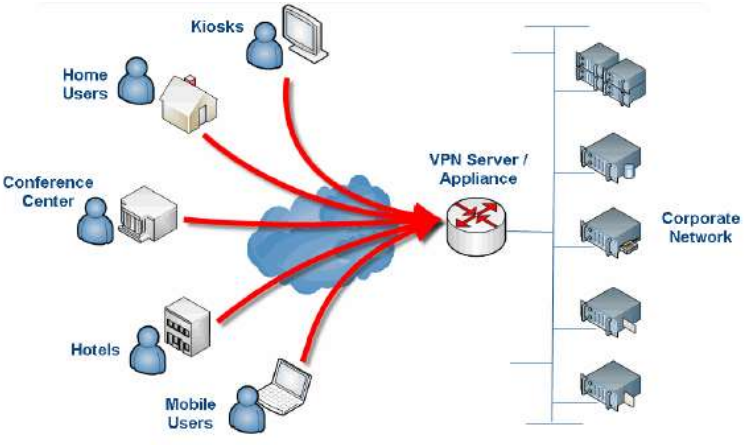


Fig. Host to gateway VPN

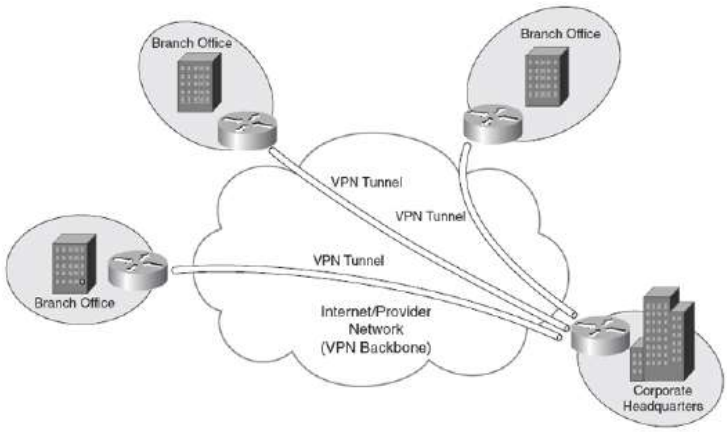


Fig Site to site VPN

- Gateway to Gateway/ Site to Site VPN
  - A Site-to-Site VPN is also called as Router-to-Router VPN and is mostly used in the corporates. Companies, with offices in different geographical locations, use Site-to-site VPN to connect the network of one office location to the network at another office location. When multiple offices of the same company are connected using Site-to-Site VPN type, it is called as **Intranet based VPN**. When companies use Site-to-site VPN type to connect to the office of another company, it is called as **Extranet based VPN**. Basically, Site-to-site VPN create a virtual bridge between the networks at geographically distant offices and connect them through the Internet and maintain a secure and private communication between the networks.
  - Since Site-to-site VPN is based on Router-to-Router communication, in this VPN type one router acts as a VPN Client and another router as a VPN Server. The communication between the two routers starts only after an authentication is validated between the two.

Tunneling protocols for VPN:

The above two VPN types are based on different VPN security protocols. Each of these VPN protocols offer different features and levels of security, and are explained below: -

1. Internet Protocol Security or IPSec:

Internet Protocol Security or IPSec is used to *secure Internet communication across an IP network.* IPSec secures Internet Protocol communication by *authenticating the session and encrypts each data packet* during the connection.

IPSec operates in two modes, *Transport mode and Tunneling mode*, to protect data transfer between two different networks. The transport mode *encrypts the message in the data packet* and the tunneling mode *encrypts the entire data packet*. IPSec can also be used with other security protocols to enhance the security system.

2. Layer 2 Tunneling Protocol (L2TP):

L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is *usually combined with another VPN security protocol like IPSec to create a highly secure VPN connection*. L2TP creates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and handles secure communication between the tunnel.

3. Point – to – Point Tunneling Protocol (PPTP):

PPTP or Point-to-Point Tunneling Protocol *creates a tunnel and encapsulates the data packet.* It uses a Point-to-Point Protocol (PPP) to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the time of Windows 95. Apart from Windows, PPTP is also supported on Mac and Linux.

4. Secure Sockets Layer (SSL) and Transport Layer Security (TLS):
SSL (Secure Sockets Layer) and TLS (Transport Layer Security) *create a VPN connection where the web browser acts as the client and user access is restricted to specific applications instead of entire network*. SSL and TLS protocol is most commonly used by online shopping websites and service providers. Web browsers switch to SSL with ease and with almost no action required from the user, since web browsers come integrated with SSL and TLS. SSL connections have https in the beginning of the URL instead of http.
5. OpenVPN: OpenVPN is an *open source VPN* that is useful for *creating Point-to-Point and Site-to-Site connections.* It uses a custom security protocol based on SSL and TLS protocol.
6. Secure Shell (SSH): Secure Shell or SSH *creates the VPN tunnel through which the data transfer happens and also ensures that the tunnel is encrypted.* SSH connections are created by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

Why we need VPN ?

1. Access Full Netflix and Streaming Content from Outside the USA : *Because of copyright agreements, Netflix and Hulu and Pandora and other streaming media providers cannot broadcast all content outside of the USA*. This means: many movies and shows are blocked to users in the UK, Canada, South America, Australia, Asia, and Europe. By using a VPN service, you can manipulate your machine's IP address to be from within the USA, therein unlocking access to more Netflix and Pandora streams.
2. Download and Upload P2P Files in Privacy : A VPN can be a P2P user's best friend*. While a VPN connection will slow your bandwidth by 25% - 50%, it will cipher your file downloads, uploads, and actual IP address so that you are unidentifiable by authorities.*
3. Use Public or Hotel Wi-Fi in Confidence : *If you log into a public wi-fi network and then connect to a personal VPN, all of your hotspot web use will then be encrypted and hidden from prying eyes.* If you are a traveler or a user who is regularly using public wireless, then a VPN is a very wise investment in privacy.
4. Break Out of a Restrictive Network at Work/School : A VPN connection will *allow you to 'tunnel out' of a restrictive network and connect to otherwise-restricted websites and webmail services.*
5. Bypass the Country's Web Censorship and Content Surveillance : If you live in restrictive countries, connecting to a VPN server will enable you to 'tunnel out' of the censorship restrictions and access the full World Wide Web.
6. Wrap Your VOIP Phone Calls : Voice-over-IP (internet telephoning) is relatively easy to listen on. Even intermediate-level hackers can listen in to your VOIP calls. If you regularly use VOIP services like Skype, Lync, or online voice chatting, definitely consider implementing a VPN connection. The monthly cost will be higher, and the VOIP speed will be slower with a VPN, but personal privacy is invaluable.
7. Use Search Engines Without Having Your Searches Logged : Like it or not, Google, Bing, and other search engines will catalog every web search you perform. Your online search choices are then attached to your computer's IP address and are subsequently used to customize the advertising and future searches for your machine.
8. Watch Home-Specific Broadcasts While You Are Traveling : By employing a VPN tunnel connection, you can force your borrowed connection to access your home country as if you were physically there, therein enabling your favorite football feeds and TV and newscasts.
9. A personal VPN connection is the best choice for manipulating your IP address and rendering you untraceable.
10. Because We Believe Privacy Is a Basic Right

Case of VPN Tunneling:

The accompanying strides represent the standards of a VPN customer server association in basic terms;
Accept a remote host with open IP address 1.2.3.4 wishes to associate with a server found inside an organization system. The server has inside location 192.168.1.10 and is not reachable openly. Prior to the customer can achieve this server, it needs to experience a VPN server/firewall gadget that has open IP address 5.6.7.8 and an interior location of 192.168.1.1. All information between the customer and the server should be kept private; thus, a protected VPN is utilized.

- The VPN customer associates with a VPN server by means of an outer system interface.
- The VPN server allocates an IP location to the VPN customer from the VPN server's subnet. The customer gets inward IP address 192.168.1.50, for instance, and makes a virtual system interface through which it will send encoded parcels to the next passage endpoint (the gadget at the flip side of the passage). (This interface likewise gets the location 192.168.1.50.)
- When the VPN customer wishes to speak with the organization server, it readies a bundle tended to 192.168.1.10, encodes it and exemplifies it in an external VPN parcel, say an IPSec bundle. This parcel is then sent to the VPN server at IP address 5.6.7.8 over general society Internet. The inward parcel is scrambled so that regardless of the possibility that somebody catches the bundle over the Internet, they can't get any data from it.
- When the bundle comes to the VPN server from the Internet, the VPN server unencapsulates the inward parcel, unscrambles it, observes the destination location to be 192.168.1.10, and advances it to the proposed server at 192.168.1.10.
- After some time, the VPN server gets an answer parcel from 192.168.1.10, planned for 192.168.1.50. The VPN server counsels its directing table, and sees this parcel is planned for a remote host that must experience VPN.

- The VPN server encodes this answer parcel, exemplifies it in a VPN bundle and sends it out over the Internet. The internal scrambled bundle has source address 192.168.1.10 and destination address 192.168.1.50. The external VPN parcel has source address 5.6.7.8 and destination address 1.2.3.4.
- The remote host gets the bundle. The VPN customer unencapsulates the internal parcel, unscrambles it, and passes it to the fitting programming at upper layers.