Application server

Freeze Time
Learning

Contents

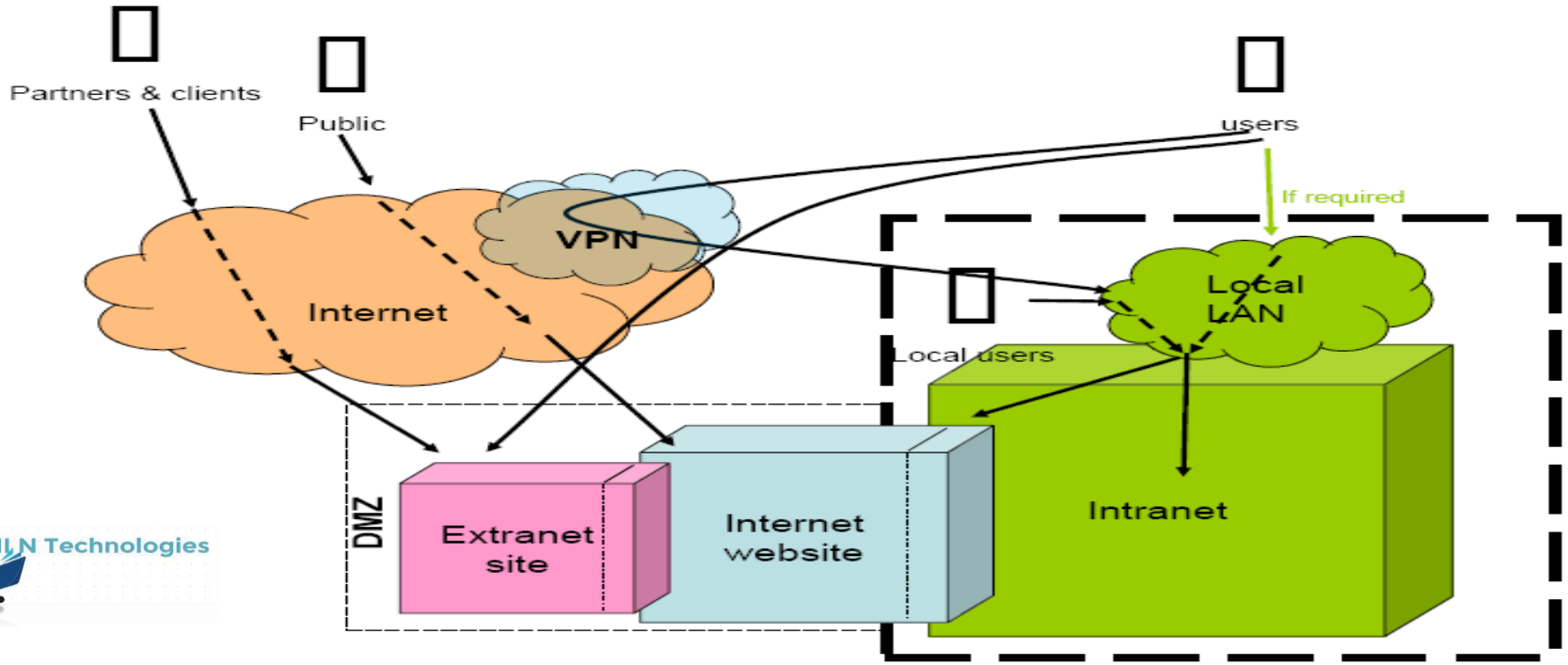
- Introduction
- Internet Vs Intranet Vs Extranet
- Web Server
- How Web Server Works
- Application Server
- Web Server & Application Server Communication
- Firewall
- DMZ (Demilitarized Zone)
- Simple Network Firewall Architecture
- Virtual Private Network (VPN)

Internet Vs Intranet Vs Extranet

Internet is worldwide, and can be accessed from any computer with an internet connection.

Intranet is like local internet, i.e. can only be accessed on a web of computers, like a business or a school. Things on the intranet can sometimes be accessed via the internet with the help of VPN. Then what is preventing external users from hitting the Intranet sites…. there comes the role of “Firewall”. We will cover about Firewall in coming slides…..

Extranet is a portion of an organization's Intranet (called DMZ) that is made accessible to authorized outside users without full access to an entire organization's intranet.



Web Server

A web server is a piece of software that enables a website to be viewed using HTTP. HTTP (Hyper Text Transfer Protocol) is the key protocol for the transfer of data on the web.

Web Server serves static HTML pages or gifs, jpegs, etc., and can also run code written in CGI, JSP etc.

Web Server Examples:

Apache HTTP Server, Microsoft IIS, iPlanet, Sun One Web Server

Basic Process

Application Server

An application server is a server program in a computer in a distributed network that provides the business logic for an application program. The application server is frequently viewed as part of a three-tier application, consisting of a graphical user interface (GUI) server, an application (business logic) server, and a database and transaction server (An Application Server is used to run business logic or dynamically generated presentation code)

• A first-tier, front-end, Web browser-based graphical user interface, usually at a personal computer or workstation

• A middle-tier business logic application or set of applications, possibly on a local area network or intranet server

• A third-tier, back-end, database and transaction server, sometimes on a mainframe or large server

Examples for Application Servers:

JBoss, BEA Weblogic, IBM Websphere, Tomcat

How Web Server Works?

If you want to get into a bit more detail on the process of getting a Web page onto your computer screen, here are the basic steps that will occur in the background:

Basically URL has three parts:
The protocol ("http")
The server name ("www.gepower.com")
The file name ("index.htm")

The browser communicated with a name server to translate the server name \ "www.gepower.com" into an IP Address, which it uses to connect to the server machine.

The browser then formed a connection to the server at that IP address on port 80.

Following the HTTP protocol, the browser sent a GET request to the server, asking for the file "http://www.gepower.com/index. htm." (Note that cookies may be sent from browser to server with the GET request)

The server then sent the HTML text for the Web page to the browser. (Cookies may also be sent from server to browser in the header for the page.)
The browser read the HTML tags and formatted the page onto your screen.

Web Server – App Server Communication

The following steps explain how a web server and web application server work together to process a page request:

❖ The user requests a page by typing a URL in a browser, and the web server receives the request.

❖ The web server looks at the file extension to determine whether a web application server must process the page. Then, one of the following actions occur:

❖ If the user requests a file that is a simple web page (often one with an HTM or HTML extension), the web server fulfills the request and sends the file to the browser.

❖ If the user requests a file that is a page that a web application server must process (one with a CFM, CFML, or CFC extension for Cold Fusion requests), the web server passes the request to the web application server. The web application server processes the page and sends the results to the web server, which returns those results to the browser.

Firewall

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

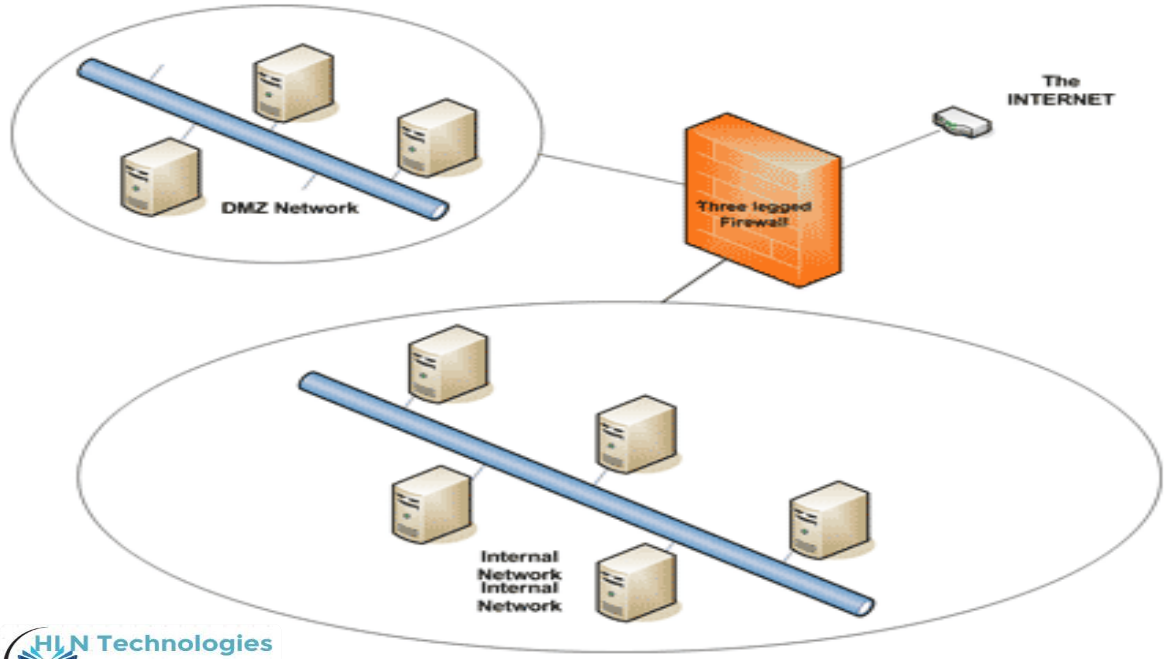
Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

DMZ (Demilitarized Zone)

In computer security, a demilitarized zone, named after the military usage of the term and normally abbreviated to DMZ; also known as a Data Management Zone or Demarcation Zone or Perimeter Network, is a physical or logical sub network that contains and exposes an organization's external services to a larger, untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network.

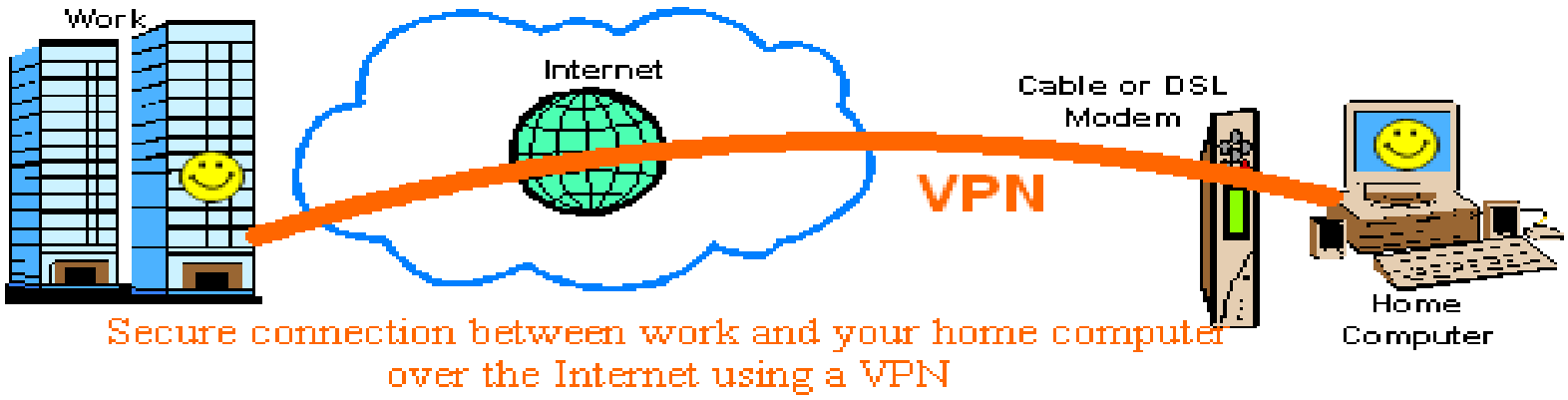
Simple Firewall Network Architecture



VPN – Virtual Private Network

A VPN is a secure, private communication tunnel between `two or more devices across a public network (like the Internet). These VPN devices can be either a computer running VPN software or a special device like a VPN enabled router. It allows your home computer to be connected to your office network or can allow two home computers in different locations to connect to each over the Internet.

Even though a VPN's data travels across a public network like the Internet, it is secure because of very strong encryption, data hacking is impossible. In addition, VPN's monitor their traffic in very sophisticated ways that ensure packets never get altered while traveling across the public network. Encryption and data verification is very CPU intensive.



NAS – Network Attached Storage

A NAS unit is essentially a self-contained computer connected to a network, with the sole purpose of supplying file-based data storage services to other devices on the network. The operating system and other software on the NAS unit provide the functionality of data storage, file systems, and access to files, and the management of these functionalities. The unit is not designed to carry out general-purpose computing tasks, although it may technically be possible to run other software on it. NAS units usually do not have a keyboard or display, and are controlled and configured over the network, often by connecting a browser to their network address.

Uses

NAS is useful for more than just general centralized storage provided to client computers in environments with large amounts of data. NAS can enable simpler and lower cost systems such as load-balancing and fault-tolerant email and web server systems by providing storage services.

Drawbacks

Due to the multiprotocol, and the reduced CPU and OS layer, the NAS has its limitations compared to the DAS/SAN systems. If the NAS is occupied with too many users, too many I/O operations, or CPU processing power that is too demanding, the NAS reaches its limitations. A server system is easily upgraded by adding one or more servers into a cluster, so CPU power can be upgraded, while the NAS is limited to its own hardware, which is in most cases not upgradeable

SAN – Storage Area Network

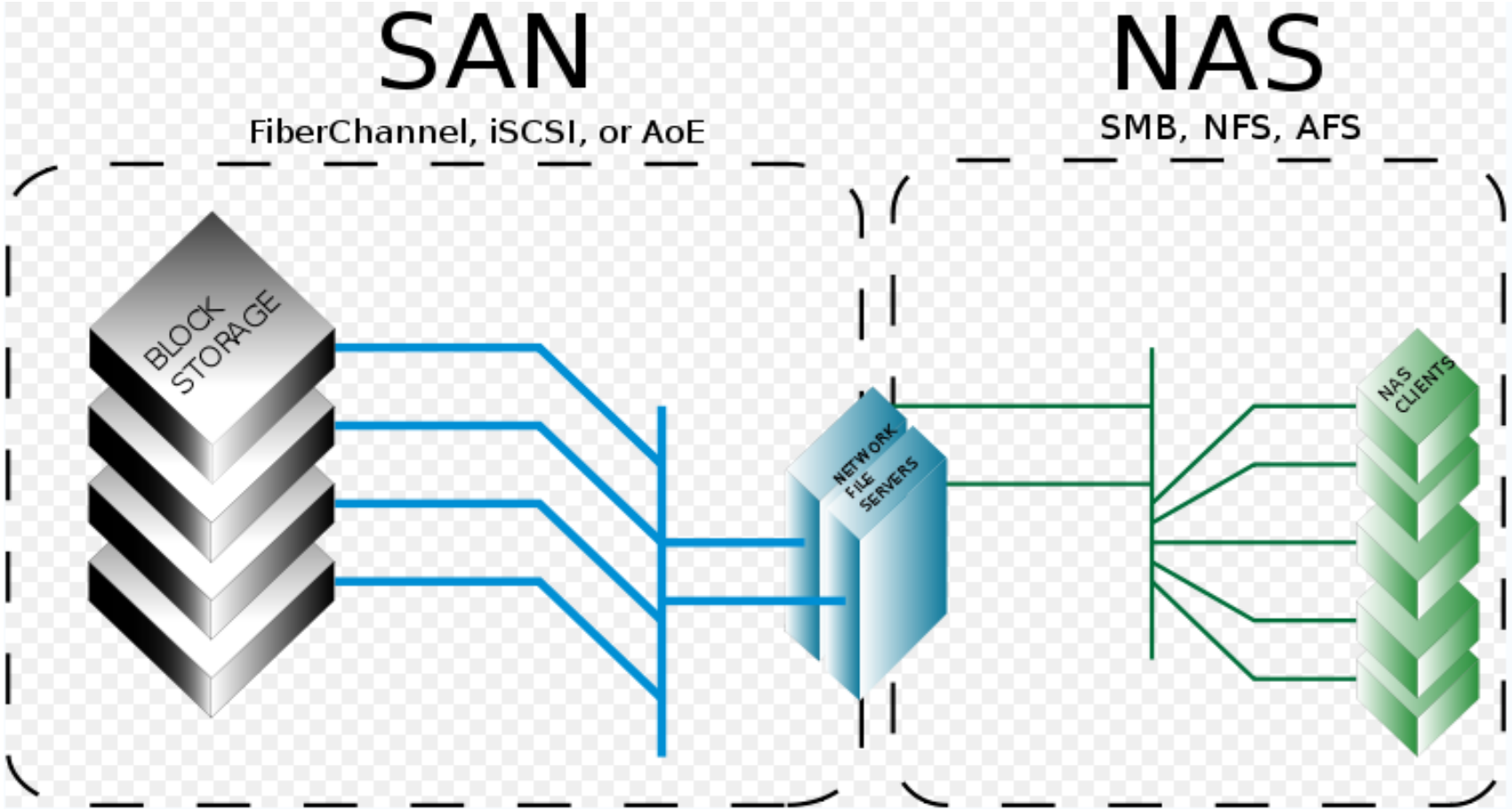
A storage area network (SAN) is an architecture to attach remote computer storage devices (such as disk arrays, tape libraries, and optical jukeboxes) to servers in such a way that the devices appear as locally attached to the operating system. Although the cost and complexity of SANs are dropping, they are uncommon outside larger enterprises.

DAS – Direct Attached Storage

Direct-attached storage (DAS) refers to a digital storage system directly attached to a server or workstation, without a storage network in between...

NAS Vs SAN

A NAS is a single storage device that operate on data files, while a SAN is a local network of multiple devices that operate on disk blocks.



Thank You

Catch you all with another document soon……