**Windows Application Firewall and**

**Unified Threat Management**

**Submitted in Partial Fulfillment of the Requirements**

**For the Award**

**Of**

**Bachelor of Technology**

**In**

**Computer Science**

**Guide : Submitted By:**

**\*Member1\* \*Member2\***

**\*Member3\* \*Member4\***



**Computer Science Department**

**\*College Name\***

**CHAPTER-1**

INTRODUCTION TO NETWORKING

* **WHAT IS A NETWORK?**
* **NETWORK TOPOLGY**
* **THE OSI MODEL**
* **LAYERS OF OSI MODELS**
* **SOME POPULAR NETWORKS**
* **UUCP**
* **THE INTERNET**
* **TCP/IP MODEL**
* **UNDERSTANDING TCP**
* **IP ADDRESS : NETWORK AND HOSTS**
* **UNDERSTANDING UDP**
* **TYPES AND SOURCES OF NETWORK THREATS**
* **DENIAL-OF-SERVICE**
* **UNAUTHORIZED ACCESS**

**WHAT IS A NETWORK?**

A network consists of two or more computers (nodes) that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

Two very common types of networks include:

* **Local Area Network (LAN)**
* **Wide Area Network (WAN)**
* **Local Area Network**

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building.

Computers connected to a network are broadly categorized as servers or workstations. Servers are generally not used by humans directly, but rather run continuously to provide "services" to the other computers (and their human users) on the network. Services provided can include printing and faxing, software hosting, file storage and sharing, messaging, data storage and retrieval, complete access control (security) for the network's resources, and many others.

On a single LAN, computers and servers may be connected by cables or wirelessly. Wireless access to a wired network is made possible by wireless access points (WAPs). These WAP devices provide a bridge between computers and networks. A typical WAP might have the theoretical capacity to connect hundreds or even thousands of wireless users to a network, although practical capacity might be far less.

Nearly always servers will be connected by cables to the network, because the cable connections remain the fastest. Workstations which are stationary (desktops) are also usually connected by a cable to the network, although the cost of wireless adapters has dropped to the point that, when installing workstations in an existing facility with inadequate wiring, it can be easier and less expensive to use wireless for a desktop.

* **Wide Area Network**

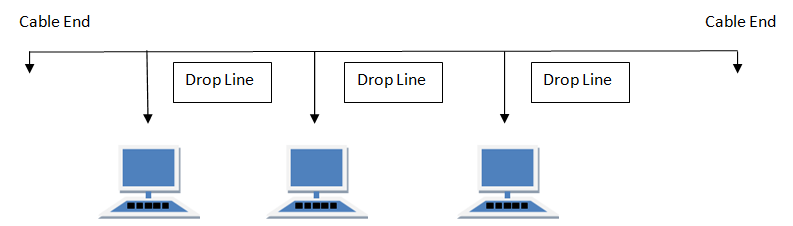
Wide Area Networks (WANs) connect networks in larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of global network.

Using a WAN, schools in Florida can communicate with places like Tokyo in a matter of seconds, without paying enormous phone bills. Two users a half-world apart with workstations equipped with microphones and a webcams might teleconference in real time. A WAN is complicated. It uses multiplexers, bridges, and routers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN.

**TYPES OF NETWORK TOPOLOGY**

Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

**BUS TOPOLOGY**

Bus topology is a network type in where every computer and network device is connected to single cable.

**Features of Bus Topology**

1. It transmits data only in one direction.
2. Every device is connected to a single cable

**Advantages of Bus Topology**

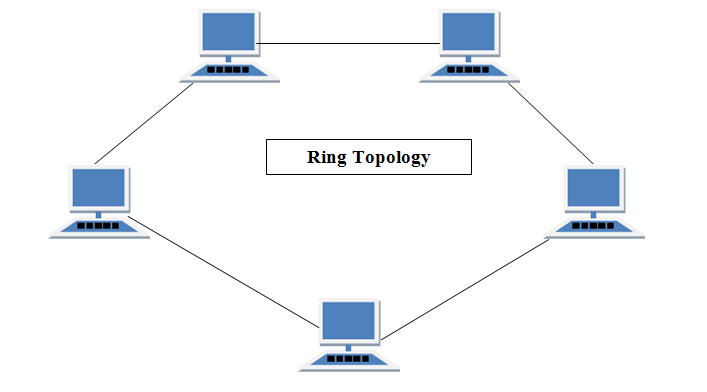
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

**Disadvantages of Bus Topology**

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

**RING TOPOLOGY**

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



**Features of Ring Topology**

1. A number of repeaters are used and the transmission is unidirectional.
2. Date is transferred in a sequential manner that is bit by bit.

**Advantages of Ring Topology**

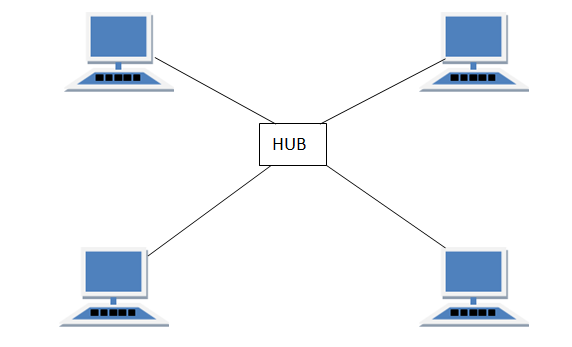
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

**Disadvantages of Ring Topology**

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

**STAR TOPOLOGY**

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



**Features of Star Topology**

1. Every node has its own dedicated connection to the hub.
2. Acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

**Advantages of Star Topology**

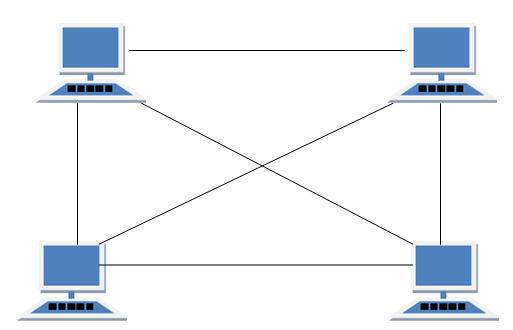
1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed rest of the nodes can work smoothly.

**Disadvantages of Star Topology**

1. Cost of installation is high.
2. Expensive to use.
3. If the hub is affected then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

**MESH TOPOLOGY**

It is a point-to-point connection to other nodes or devices. Traffic is carried only between two devices or nodes to which it is connected. Mesh has n (n-2)/2 physical channels to link hn devices.



**Features of Mesh Topology**

1. Fully connected.
2. Robust.
3. Not flexible.

**Advantages of Mesh Topology**

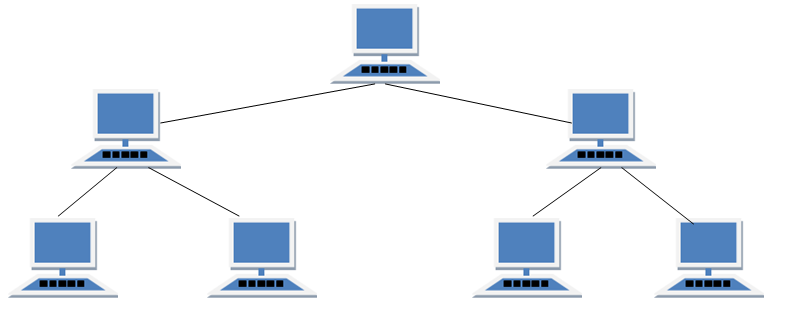
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

**Disadvantages of Mesh Topology**

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

**TREE TOPOLOGY**

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



**Features of Tree Topology**

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

**Advantages of Tree Topology**

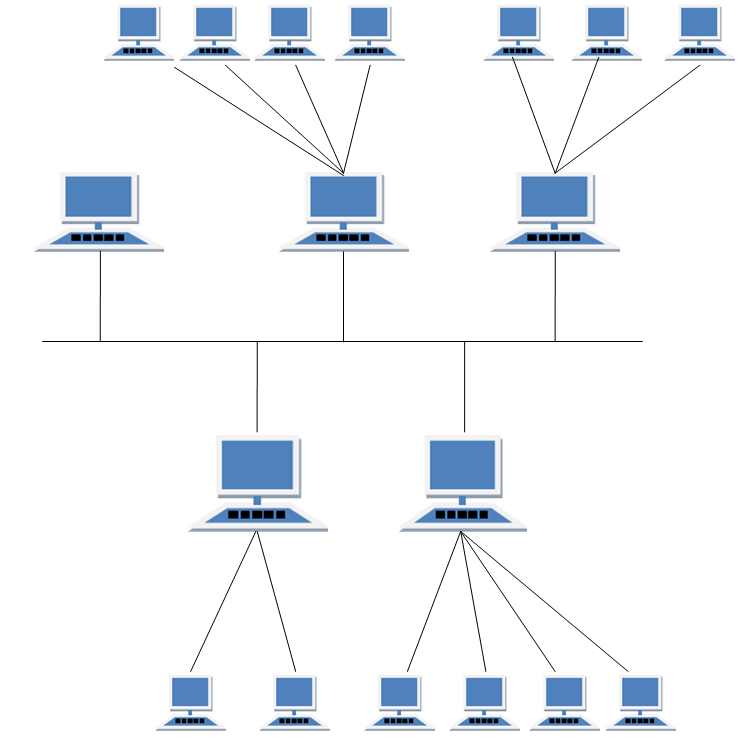
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

**Disadvantages of Tree Topology**

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

**HYBRID TOPOLOGY**

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



**Features of Hybrid Topology**

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

**Advantages of Hybrid Topology**

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

**Disadvantages of Hybrid Topology**

1. Complex in design.
2. Costly.

**THE OSI MODEL**

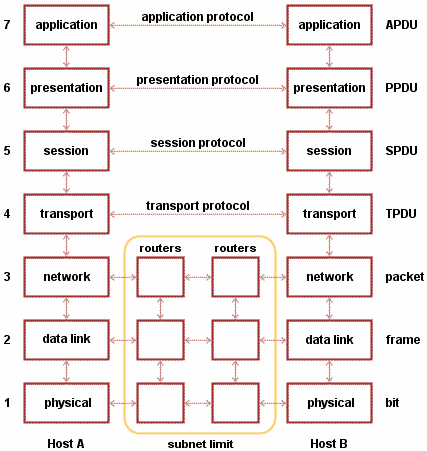
OSI (Open Systems Interconnection) is reference model for how applications can communicate over a network. A reference model is a conceptual framework for understanding relationships. The purpose of the OSI reference model is to guide vendors and developers so the digital communication products and software programs they create will interoperate, and to facilitate clear comparisons among communications tools. Most vendors involved in telecommunications make an attempt to describe their products and services in relation to the OSI model. And although useful for guiding discussion and evaluation, OSI is rarely actually implemented, as few network products or standard tools keep all related functions together in well-defined layers as related to the model.

Developed by representatives of major computer and telecommunication companies beginning in 1983, OSI was originally intended to be a detailed specification of actual interfaces. Instead, the committee decided to establish a common reference model for which others could then develop detailed interfaces, which in turn could become standards. OSI was officially adopted as an international standard by the International Organization of Standards (ISO).

**LAYERS OF OSI MODELS**

The main concept of OSI is that the process of communication between two endpoints in a telecommunication network can be divided into seven distinct groups of related functions, or layers. Each communicating user or program is at a computer that can provide those seven layers of function. So in a given message between users, there will be a flow of data down through the layers in the source computer, across the network and then up through the layers in the receiving computer. The seven layers of function are provided by a combination of applications, operating systems, network card device drivers and networking hardware that enable a system to put a signal on a network cable or out over Wi-Fi or other wireless protocol).

The seven Open Systems Interconnection layers are:



|  |
| --- |
| * **LAYER 7: THE APPLICATION LAYER**- This is the layer at which communication partners are identified (Is there someone to talk to?), network capacity is assessed (Will the network let me talk to them right now?), and that creates a thing to send or opens the thing received. This layer is not the application itself, it is the set of services an application should be able to make use of directly, although some applications may perform application layer functions. * **LAYER 6: THE PRESENTATION LAYER-** This layer is usually part of an operating system (OS) and converts incoming and outgoing data from one presentation format to another (for example, from clear text to encrypted text at one end and back to clear text at the other).      * **LAYER 5: THE SESSION LAYER**- This layer sets up, coordinates and terminates conversations. Services include authentication and reconnection after an interruption. On the Internet, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) provide these services for most applications. * **LAYER 4: THE TRANSPORT LAYER**- This layer manages packetization of data, then the delivery of the packets, including checking for errors in the data once it arrives. On the Internet, TCP and UDP provide these services for most applications as well. * **LAYER 3: THE NETWORK LAYER-** This layer handles the addressing and routing of the data (sending it in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level). IP is the network layer for the Internet. * **LAYER 2: THE DATA-LINK LAYER-** This layer sets up links across the physical network, putting packets into network frames. This layer has two sub-layers, the Logical Link Control Layer and the Media Access Control Layer. Ethernet is the main data link layer in use. * **LAYER 1: THE PHYSICAL LAYER-** This layer conveys the bit stream through the network at the electrical, optical or radio level. It provides the hardware means of sending and receiving data on a carrier network. The physical layer consists of the basic networking hardware transmission technologies of a network. It is a fundamental layer underlying the logical data structures of the higher level functions in a network. Due to the plethora of available hardware technologies with widely varying characteristics, this is perhaps the most complex layer in the OSI architecture. |

**SOME POPULAR NETWORKS**

Over the last 25 years, a number of networks and network protocol have been defined and used. We’re going to look at two of these networks, both of which are “public” networks. Anyone can connect to either of these networks, or they can use types of networks to connect their own hosts (computers) together, without connecting to the public networks. Each type takes a very different approach to providing network services. The following two networks are the example of such kind of popular network.

**UUCP**

UUCP (UNIX-to-UNIX Copy Protocol) is a set of UNIX programs for copying (sending) files between different UNIX systems and for sending commands to be executed on another system. The main UUCP commands (each supported by a UUCP program) are:

* **UUCP,** which requests the copying of a specific file to another specified system
* **UUX**, which sends a UNIX command to another system where it is queued for execution
* **UUCICO**, which runs on a UNIX system as the program that carries out the copying and initiates execution of the commands that have been sent. Typically, this program is run at various times of day; meanwhile, the copy (uucp) and command (uux) requests are queued until the uucico program is run.
* **UUXQT**, which executes the commands sent by uux, usually after being started by the uucico program

The **UUCICO** programs are the programs that actually communicate across a network. There are several network protocols (variations on packet size and error-checking) that can be used by uucico programs, depending on the kinds of carrier networks being used.

**THE INTERNET**

The Internet is a global network connecting millions of computers. More than 190 countries are linked into exchanges of data, news and opinions. According to Internet Live Stats, as of December 30, 2014 there was an estimated 3,037,608,300 Internet users worldwide. The number of Internet users represents nearly 40 percent of the world's population. The largest number of Internet users by country is China, followed by the United States and India.

In September 2014, the total number of websites with a unique hostname online exceeded 1 billion. This is an increase from one website (info.cern.ch) in 1991.

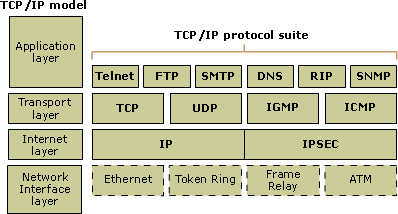
The Internet is decentralized

Unlike online services, which are centrally controlled, by design, the Internet is decentralized. Each Internet computer, called a host, is independent. Operators can choose which Internet services to use and which local services to make available to the global Internet community. Remarkably, this anarchy by design works exceedingly well. There are a variety of ways to access the Internet. Most online services offer access to some Internet services. It is also possible to gain access through a commercial Internet Service Provider (ISP).

**TCP/IP MODEL**

TCP/IP is based on a four-layer reference model. All protocols that belong to the TCP/IP protocol suite are located in the top three layers of this model.

As shown in the following illustration, each layer of the TCP/IP model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) reference model proposed by the International Standards Organization (ISO).



The types of services performed and protocols used at each layer within the TCP/IP model are described in more detail in the following table.

### 

|  |  |  |
| --- | --- | --- |
| **Layer** | **Description** | **Protocols** |
| Application | Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network. | HTTP, Telnet, FTP, TFTP, SNMP  DNS, SMTP, X Windows, other application protocols |
| Transport | Provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data. | TCP, UDP, RTP |
| Internet | Packages data into IP datagram, which contain source and destination address information that is used to forward the datagram between hosts and across networks. Performs routing of IP datagram. | IP, ICMP, ARP, RARP |
| Network interface | Specifies details of how data is physically sent through the network, including how bits are electrically signalled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fibre, or twisted-pair copper wire. | Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35 |

**UNDERSTANDING TCP**

TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet. TCP is defined by the Internet Engineering Task Force (IETF) in the Request for Comment (RFC) standards document number 793.

TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control, and—because it is meant to provide error-free data transmission—handles retransmission of dropped or garbled packets as well as acknowledgement of all packets that arrive. In the Open Systems Interconnection (OSI) communication model, TCP covers parts of Layer 4, the Transport Layer, and parts of Layer 5, the Session Layer.

For example, when a Web server sends an HTML file to a client, it uses the HTTP protocol to do so. The HTTP program layer asks the TCP layer to set up the connection and send the file. The TCP stack divides the file into packets, numbers them and then forwards them individually to the IP layer for delivery. Although each packet in the transmission will have the same source and destination IP addresses, packets may be sent along multiple routes. The TCP program layer in the client computer waits until all of the packets have arrived, then acknowledges those it receives and asks for the retransmission on any it does not (based on missing packet numbers), then assembles them into a file and delivers the file to the receiving application.

**IP ADDRESSES: NETWORKS AND HOSTS**

An IP address is a 32-bit number that uniquely identifies a host (computer or other device, such as a printer or router) on a TCP/IP network.

IP addresses are normally expressed in dotted-decimal format, with four numbers separated by periods, such as 192.168.123.132. To understand how subnet masks are used to distinguish between hosts, networks, and sub networks, examine an IP address in binary notation.

For a TCP/IP wide area network (WAN) to work efficiently as a collection of networks, the routers that pass packets of data between networks do not know the exact location of a host for which a packet of information is destined. Routers only know what network the host is a member of and use information stored in their route table to determine how to get the packet to the destination host's network. After the packet is delivered to the destination's network, the packet is delivered to the appropriate host.

For this process to work, an IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address.

**UNDERSTANDING UDP**

UDP (User Datagram Protocol) is an alternative communications protocol to Transmission Control Protocol (TCP) used primarily for establishing low-latency and loss tolerating connections between applications on the Internet. Both UDP and TCP run on top of the Internet Protocol (IP) and are sometimes referred to as UDP/IP or TCP/IP. Both protocols send short packets of data, called datagram.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

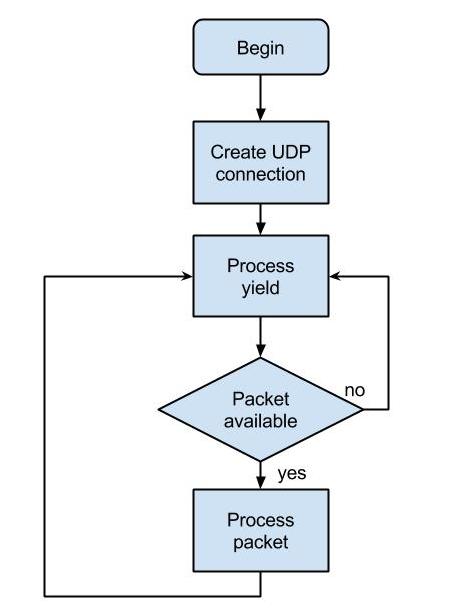
TCP has emerged as the dominant protocol used for the bulk of Internet connectivity owing to services for breaking large data sets into individual packets, checking for and resending lost packets and reassembling packets into the correct sequence. But these additional services come at a cost in terms of additional data overhead, and delays called latency.

In contrast, UDP just sends the packets, which means that it has much lower bandwidth overhead and latency. But packets can be lost or received out of order as a result, owing to the different paths individual packets traverse between sender and receiver.

UDP is an ideal protocol for network applications in which perceived latency is critical such as gaming, voice and video communications, which can suffer some data loss without adversely affecting perceived quality. In some cases, forward error correction techniques are used to improve audio and video quality in spite of some loss.

UDP can also be used in applications that require lossless data transmission when the application is configured to manage the process of retransmitting lost packets and correctly arranging received packets. This approach can help to improve the data transfer rate of large files compared with TCP.

In the Open Systems Interconnection (OSI) communication model, UDP, like TCP, is in layer 4, the Transport Layer. UDP works in conjunction with higher level protocols to help manage data transmission services including Trivial File Transfer Protocol (TFTP), Real Time Streaming Protocol (RTSP), Simple Network Protocol (SNP) and Domain Name System (DNS) lookups.



**TYPES AND SOURCES OF NETWORK THREATS**

**DENIAL-OF-SERVICE**:

DoS (Denial-of-Service) attacks are the most difficult to address. These are the nastiest, because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker, without also refusing legitimate requests for service.

The premise of a DoS attack is simple: it sends more requests to the machine than it can handle. The attacker's program simply makes a connection on some service port, perhaps forging the packet's header information that says where the packet came from, and then dropping the connection.

**UNAUTHORIZED ACCESS**:

``Unauthorized access'' is a very high-level term that can refer to a number of different sorts of attacks. The goal of these attacks is to access some resource that our machine should not provide the attacker. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator.

**1. Executing Commands Illicitly**

There are two main classifications of the severity of this problem: normal user access, and administrator access. A normal user can do a number of things on a system (such as read files, mail them to other people, etc.) that an attacker should not be able to do. This might, then, be all the access that an attacker needs. On the other hand, an attacker might wish to make configuration changes to a host. In this case, the attacker will need to gain administrator privileges on the host.

**2. Confidentiality Breaches**

We need to examine the threat model: what is it that we are trying to protect ourselves against? There is certain information that could be quite damaging if it fell into the hands of a competitor, an enemy, or the public. In these cases, it's possible that compromise of a normal user's account on the machine can be enough to cause damage (perhaps in the form of PR, or obtaining information that can be used against the company, etc.)

While many of the perpetrators of these sorts of break-ins are merely thrill-seekers interested in nothing more than to see a shell prompt for our computer on their screen, there are those who are more malicious.

**3. Destructive Behaviour**

Among the destructive sorts of break-ins and attacks, there are two major categories.

a. Data Diddling:

This type of attack is likely the worst sort, since the fact of a break-in might not be immediately obvious. Perhaps the numbers in our spreadsheets or the dates in our projections and plans might be changed.

b. Data Destruction:

Some of those perpetrate attacks are simply twisted jerks who like to delete things. In these cases, the impact on our computing capability -- and consequently our business -- can be nothing less than if a fire or other disaster caused our computing equipment to be completely destroyed.

**CHAPTER-3**

WEB APPLICATION FIREWALL

* **WHAT IS A WAF?**
* **CONFIGURATION OF WAF**
* **GATEWAY MODE**
* **BRIDGE MODE**
* **ATTACKS PREVENTED BY WAF**
* **SQL INJECTION**
* **CROSS SITTE SCRIPTING**
* **DOS AND DDOS ATTACKS**
* **SESSION HIJACKING**
* **IP SPOOFING**

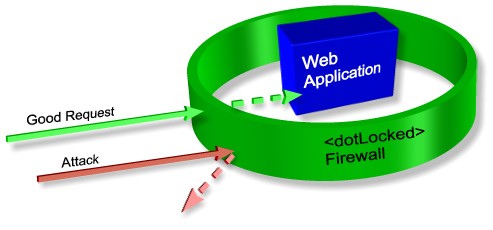
**WHAT IS WAF?**

A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

WAF solutions are capable of preventing attacks that network firewalls and intrusion detection systems can't, and they do not require modification of application source code.

It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall. The application firewall is typically built to control all network traffic on any OSI layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall, which is - without additional software - unable to control network traffic regarding a specific application.

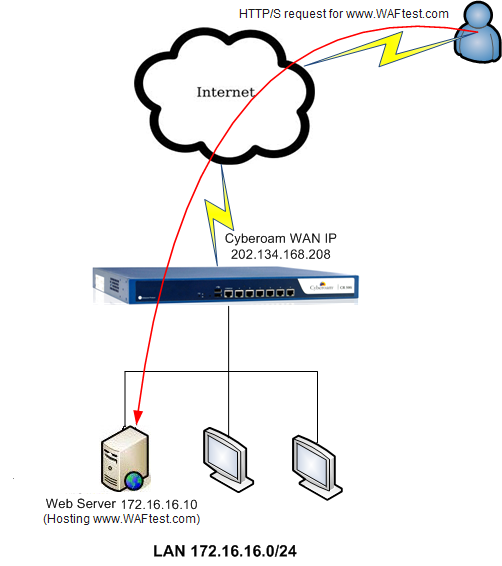
Web application firewall is a computer networking firewall operating at the application layer of a protocol stack and is also known as a proxy-based or reverse-proxy firewall. Application firewalls specific to a particular kind of network traffic may be titled with the service name, such as a web application firewall. They may be implemented through software running on a host or a stand-alone piece of network hardware. Often, it is a host using various forms of proxy servers to proxy traffic before passing it on to the client or server. Because it acts on the application layer, it may inspect the contents of traffic, blocking specified content, such as certain websites, viruses, or attempts to exploit known logical flaws in client software.

****

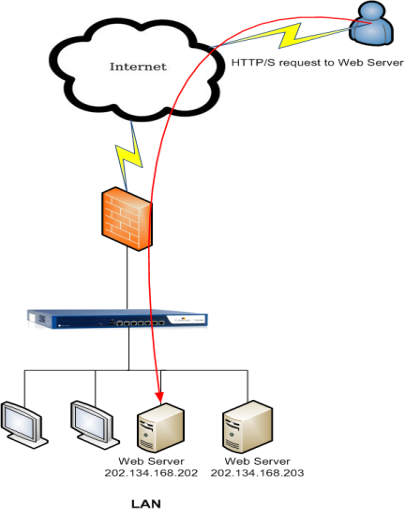
**CONFIGURATION OF WEB APPLICATION FIREWALL**

Web Application Firewall (WAF) feature protects Web Server(s) deployed in a network and related applications from any underlying vulnerability exploit. It protects applications accessed via HTTP and HTTPS at the Layer 7 - Application Layer. Besides Layer 7 based attacks, the Web Server is safeguarded against cookie tampering, forceful browsing and hidden field tampering. The WAF also mitigates "user-induced" vulnerability in configured applications or in custom-developed code that leaves Web applications open to attacks, such as cross-site scripting, directory traversal and forced URL browsing.

**CONFIGURE WAF WHEN IT IS IN GATEWAY MODE**

As shown in the diagram given below, it is deployed in Gateway Mode and WAF protection is enabled. The web server is located in the LAN zone behind the WAF device. A user on the Internet should be able to access the website http://www.WAFtest.com hosted on internal web server (172.16.16.10) using public IP address, i.e., Its WAN IP (202.134.168.208).

**CONFIGURE WAF WHEN ITIS IN BRIDGE MODE**

As shown in the diagram given below, it is deployed in Bridge Mode and WAF protection is enabled. The web server is located behind the WAF device. A user on the Internet should be able to access the website http://www.WAFtest.com hosted on Web Server using its public IP address (202.134.168.202).

**ATTACKS PREVENTED BY WEB APPLICATION FIREWALL**

**1. SQL INJECTION**

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

**Threat Modelling**

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

SQL Injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. Due to the nature of programmatic interfaces available, J2EE and ASP.NET applications are less likely to have easily exploited SQL injections.

The severity of SQL Injection attacks is limited by the attacker’s skill and imagination, and to a lesser extent, defence in depth countermeasures, such as low privilege connections to the database server and so on. In general, consider SQL Injection a high impact severity.

**Description**

SQL injection errors occur when:

* Data enters a program from an untrusted source.
* The data used to dynamically construct a SQL query

The main consequences are:

* Confidentiality: Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL Injection vulnerabilities.
* Authentication: If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.
* Authorization: If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of SQL Injection vulnerability.
* Integrity: Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL Injection attack.

**2. CROSS-SITE SCRIPTING (XSS)**

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

**Description**

Cross-Site Scripting (XSS) attacks occur when:

* Data enters a Web application through an untrusted source, most frequently a web request.
* The data is included in dynamic content that is sent to a web user without being validated for malicious content.

The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash, or any other type of code that the browser may execute. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

* Stored XSS Attacks

Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information. Stored XSS is also sometimes referred to as Persistent or Type-I XSS.

* Reflected XSS Attacks

Reflected attacks are those where the injected script is reflected off the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request. Reflected attacks are delivered to victims via another route, such as in an e-mail message, or on some other web site. When a user is tricked into clicking on a malicious link, submitting a specially crafted form, or even just browsing to a malicious site, the injected code travels to the vulnerable web site, which reflects the attack back to the user’s browser. The browser then executes the code because it came from a "trusted" server. Reflected XSS is also sometimes referred to as Non-Persistent or Type-II XSS.

**3. DOS ATTACKS AND DDOS ATTACKS**

The Denial of Service (DoS) attack is focused on making a resource (site, application, server) unavailable for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others. If a service receives a very large number of requests, it may cease to be available to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources it uses.

Sometimes the attacker can inject and execute arbitrary code while performing a DoS attack in order to access critical information or execute commands on the server. Denial-of-service attacks significantly degrade the service quality experienced by legitimate users. These attacks introduce large response delays, excessive losses, and service interruptions, resulting in direct impact on availability.

**Methods of attack**

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services.

A DoS attack can be perpetrated in a number of ways. Attacks can fundamentally be classified into five families:

* Consumption of computational resources, such as bandwidth, memory, disk space, or processor time.
* Disruption of configuration information, such as routing information.
* Disruption of state information, such as unsolicited resetting of TCP sessions.
* Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

A DoS attack may include execution of malware intended to:

* Max out the processor's usage, preventing any work from occurring.
* Trigger errors in the microcode of the machine.
* Trigger errors in the sequencing of instructions, so as to force the computer into an unstable state or lock-up.
* Exploit errors in the operating system, causing resource starvation and/or thrashing, i.e. to use up all available facilities so no real work can be accomplished or it can crash the system itself
* Crash the operating system itself.

In most cases DoS attacks involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot easily be identified and to prevent filtering of the packets based on the source address.

**4. SESSION HIJACKING ATTACKS**

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user’s connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition.

The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

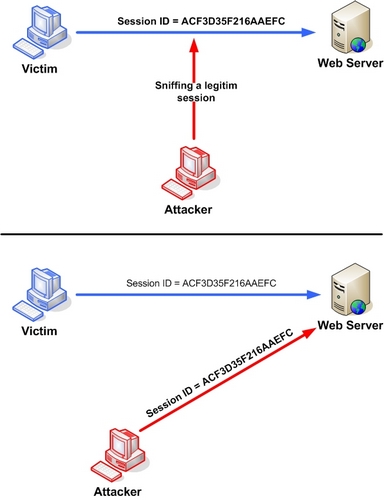
The session token could be compromised in different ways; the most common are:

* Predictable session token;
* Session Sniffing;
* Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc);
* Man-in-the-middle attack
* Man-in-the-browser attack

**Example 1**

**Session Sniffing**

In the example, as we can see, first the attacker uses a sniffer to capture a valid token session called “Session ID”, and then he uses the valid token session to gain unauthorized access to the Web Server.

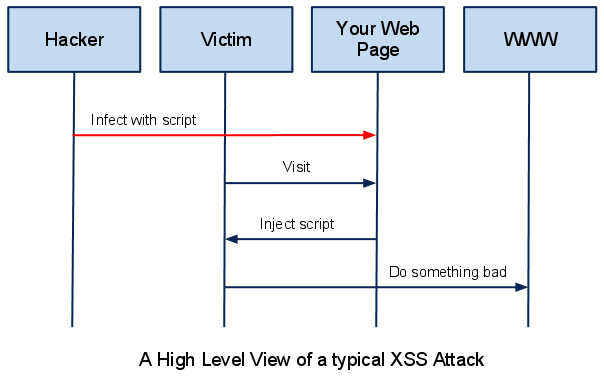


Manipulating the token session executing the session hijacking attack.

**Example 2**

**Cross-site script attack**

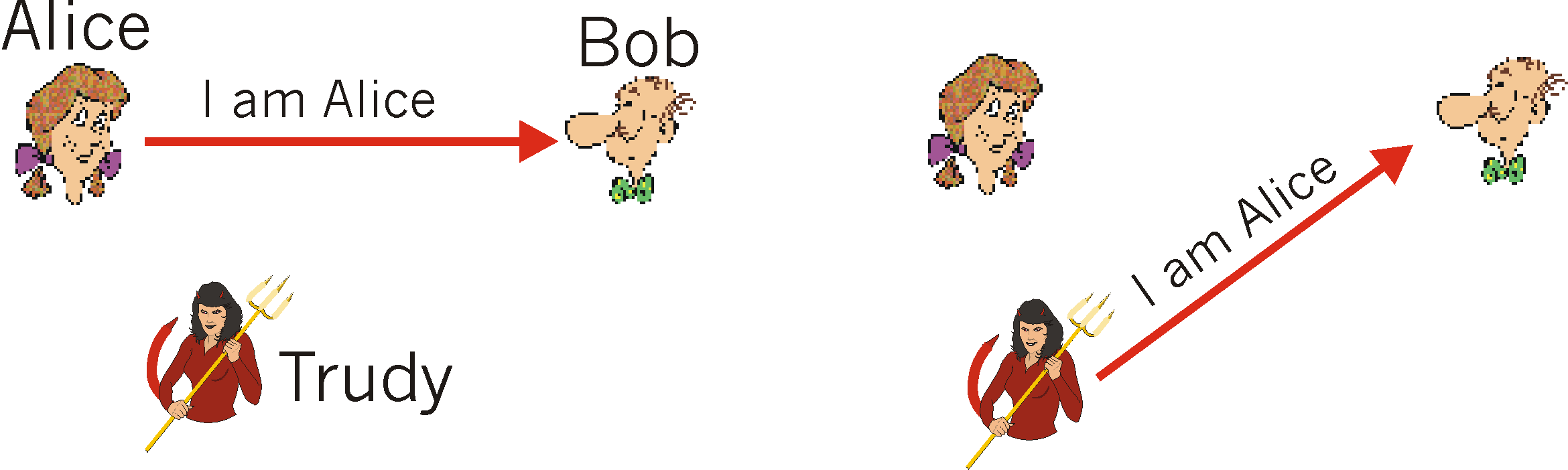
The attacker can compromise the session token by using malicious code or programs running at the client-side. The example shows how the attacker could use an XSS attack to steal the session token. If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker. The example in figure 3 uses an XSS attack to show the cookie value of the current session; using the same technique it's possible to create a specific JavaScript code that will send the cookie to the attacker.



**5. IP SPOOFING**

IP spoofing, also known as IP address forgery, is a hijacking technique in which the attacker masquerades as a trusted host to conceal his identity, hijack browsers, or gain access to a network. The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.

If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.

Web site administrators can minimize the danger that their IP addresses will be spoofed by implementing hierarchical or one-time passwords and data encryption/decryption techniques. Users and administrators can protect themselves and their networks by installation and implementation firewalls that block outgoing packets with source addresses that differ from the IP address of the user's computer or internal network.

**CHAPTER-3**

UNIFIED THREAT MANAGEMENT

* **WHAT IS A UTM?**
* **CONFIGURATION OF UTM**
* **NETWORK INTRUSION PREVENTION**
* **ANTIVIRUS**
* **ANTISPAM**
* **VPN**
* **CONTENT FILTERING**

**WHAT IS UTM?**

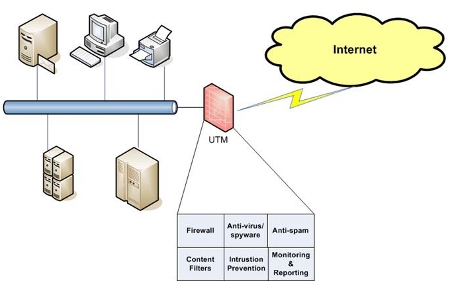
Unified threat management (UTM) is an approach to security management that allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console.

UTMs, which are typically purchased as cloud services or network appliances, provide firewall, intrusion detection, antimalware, spam and content filtering and VPN capabilities in one integrated package that can be installed and updated easily. UTMs for enterprise customers may also include more advanced features such as identity-based access control, load balancing, quality of service (QoS), intrusion prevention, SSL and SSH inspection and application awareness.

The principal advantage of a UTM product is its ability to reduce complexity. The principal disadvantage is that a UTM appliance can become a single point of failure (SPOF).

A single UTM appliance simplifies management of a company's security strategy, with just one device taking the place of multiple layers of hardware and software. Also from one single centralized console, all the security solutions can be monitored and configured. In this context, UTMs represent all-in-one security appliances that carry a variety of security capabilities including firewall, VPN, gateway anti-virus, gateway anti-spam, intrusion prevention, content filtering, bandwidth management, application control and centralized reporting as basic features.

The UTM has a customized OS holding all the security features at one place, which can lead to better integration and throughput than a collection of disparate devices. For enterprises with remote networks or distantly located offices, UTMs are a means to provide centralized security with control over their globally distributed networks.

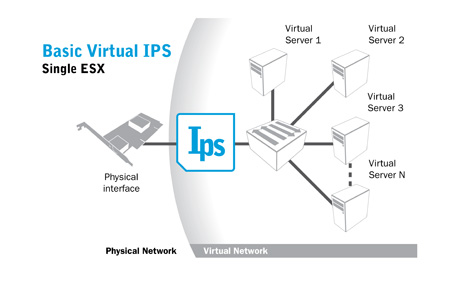


**NETWORK INTRUSION PREVENTION**

Intrusion prevention is a pre-emptive approach to network security used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator. For example, an IPS might drop a packet that it determines to be malicious and block all further traffic from that IP address or port. Legitimate traffic, meanwhile, should be forwarded to the recipient with no apparent disruption or delay of service.

According to Michael Reed of Top Layer Networks, an effective intrusion prevention system should also perform more complex monitoring and analysis, such as watching and responding to traffic patterns as well as individual packets. "Detection mechanisms can include address matching, HTTP string and substring matching, generic pattern matching, TCP connection analysis, packet anomaly detection, traffic anomaly detection and TCP/UDP port matching."

Broadly speaking, an intrusion prevention system can be said to include any product or practice used to keep attackers from gaining access to your network, such as firewalls and anti-virus software.



**ANTIVIRUS**

Antivirus (anti-virus) software is a class of program that will prevent, detect and remediate malware infections on individual computing devices and IT systems.

The label "antivirus" was originally given to programs that identified and removed a particular type of malware called a virus. Today, however, antivirus programs are useful for preventing infections caused by many types of malware, including worms, Trojan horses, rootkits, spyware, keyloggers, ransomware and adware.

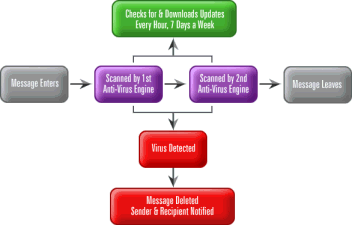
**ANTISPAM**

Anti-spam refers to services and solutions that focus on blocking and mitigating the effects of illegal emails - or spam - on email users. To achieve this objective, different types of anti-spam systems have been integrated with the email systems of many email and Internet service providers (ISP).

Modern anti-spam technology covers a broad spectrum of filters, scanners and other types of applications. Some anti-spam services work from a statistical method, while others use heuristics or predictive algorithms. To sort email in sophisticated ways, anti-spam service providers may monitor email signatures, IP addresses or other data, which reduces spam. The emergence of anti-spam software adds to the ongoing conflict between email recipients and unsolicited email senders. ISPs and email providers are working to secure legislative victories that could block certain types of email marketing. However, senders may find ways to shield a message's origins, or imitate another sender's signature or other email features. Likewise, senders may find ways to combat anti-spam tool algorithms and break through filters to reach email users.

**DIFFERENCE BETWEEN ANTISPAM AND ANTIVIRUS**

A virus is malicious software that is used with intent to destroy files, and/or make your life miserable on the computer. Spyware is known for gathering information about you and your browsing habits and sending it to a third party, Spam is that annoying e-mail you get about random things you will never use. Each anti-spam is designed to eliminate or catch these things.

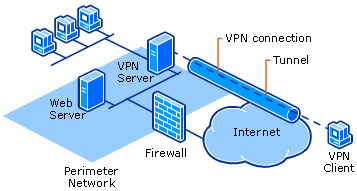


**VIRTUAL PRIVATE NETWORKING SECURITY**

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunnelling protocols, or traffic encryption. Major implementations of VPNs include OpenVPN and IPSec.

A VPN connection across the Internet is similar to a wide area network (WAN) link between websites. From a user perspective, the extended network resources are accessed in the same way as resources available within the private network. One major limitation of traditional VPNs is that they are point-to-point, and do not tend to support or connect broadcast domains. Therefore communication, software, and networking, which are based on layer 2 and broadcast packets, such as NetBIOS used in Windows networking, may not be fully supported or work exactly as they would on a real LAN. Variants on VPN, such as Virtual Private LAN Service (VPLS), and layer 2 tunnelling protocols, are designed to overcome this limitation.

VPNs allow employees to securely access their company's intranet while travelling outside the office. Similarly, VPNs securely connect geographically separated offices of an organization, creating one cohesive network. VPN technology is also used by individual Internet users to secure their wireless transactions, to circumvent geo restrictions and censorship, and to connect to proxy servers for the purpose of protecting personal identity and location.



**CONTENT FILTERING**

On the Internet, content filtering (also known as information filtering) is the use of a program to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable. Content filtering is used by corporations as part of Internet firewall computers and also by home computer owners, especially by parents to screen the content their children have access to from a computer.

Content filtering usually works by specifying character strings that, if matched, indicate undesirable content that is to be screened out. Content is typically screened for pornographic content and sometimes also for violence- or hate-oriented content. Critics of content filtering programs point out that it is not difficult to unintentionally exclude desirable content.

Content filtering and the products that offer this service can be divided into Web filtering, the screening of Web sites or pages, and e-mail filters, the screening of e-mail for spam or other objectionable content.

