Introduction to Information security

Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one. Information can be anything like Your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus, Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, online social media etc.

Why is information security important?

Whichever type of information security management provider you choose, the quality of the security measures is essential. You need to be confident that you're protected from unauthorized access and security breaches. The device and network security services should cover the following areas:

- Reducing the risk of data breaches and attacks in IT systems.
- Applying security controls to prevent unauthorized access to sensitive information.
- Preventing disruption of services, e.g., denial-of-service attacks.
- Protecting IT systems and networks from exploitation by outsiders.
- Keeping downtime to a minimum so productivity stays high.
- Ensuring business continuity through data protection of information assets.
- Providing peace of mind by keeping confidential information safe from security threats.
- information security is various measures to protect information from unauthorized persons. In the pre-digital era, people locked important documents in safes, hired security guards, and encrypted their messages on paper to protect data.
- Today, digital information is more often protected. Still, the measures are essentially the same: information security specialists create protected spaces (virtual "safes"), install security software like antivirus ("hire security guards") and use cryptographic methods to encrypt digital information.

7 Different Types of Firewalls

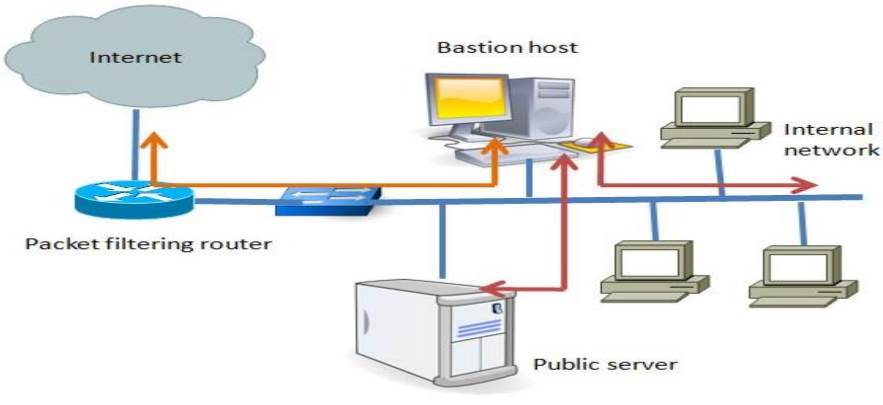
There are several types of firewalls that work on different layers of the OSI model. Depending on the kind of service and security you need for your network, you need to choose the right type of firewall. The following are the list of seven different types firewalls that are widely used for network security.

- Screened host firewalls
- Screened subnet firewalls
- Packet filter firewalls
- Stateful inspection firewalls
- Hybrid firewalls
- Proxy server firewalls
- Application level (gateway) firewalls

1. Screened host firewalls:

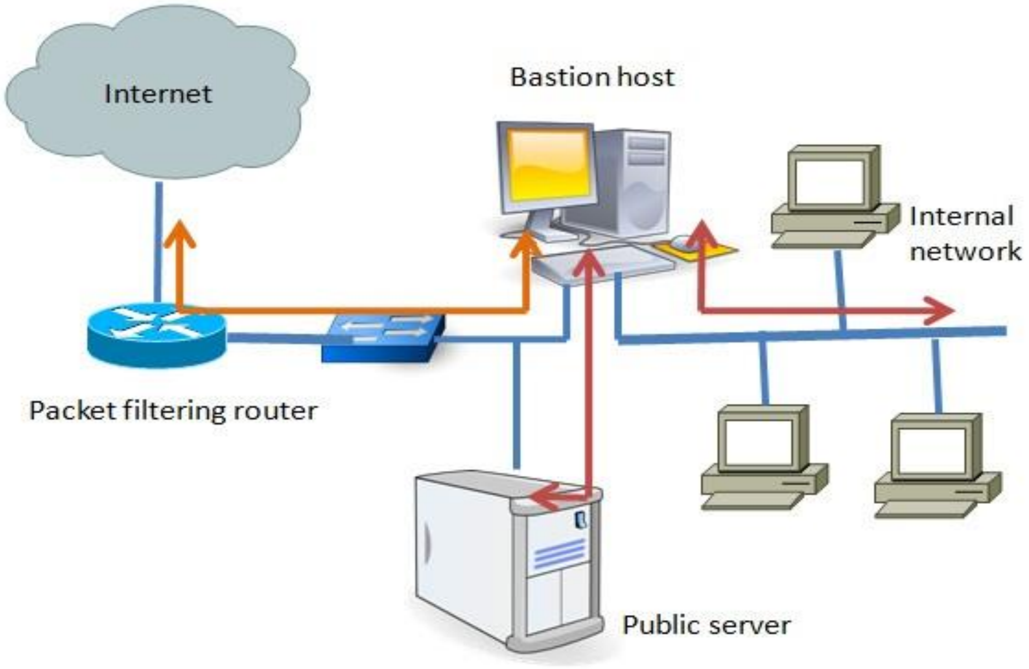
There are two types of screened host-one is single homed bastion host and the other one is dual homed bastion host**.** In case of single homed bastion host the firewall system consists of a packet filtering router and a bastion host. A bastion host is basically a single computer with high security configuration, which has the following characteristics:

- Traffic from the Internet can only reach the bastion host; they cannot reach the internal network.
- Traffic having the IP address of the bastion host can only go to the Internet. No traffic from the internal network can go to the Internet.



Screened host firewall (single-homed bastion host)

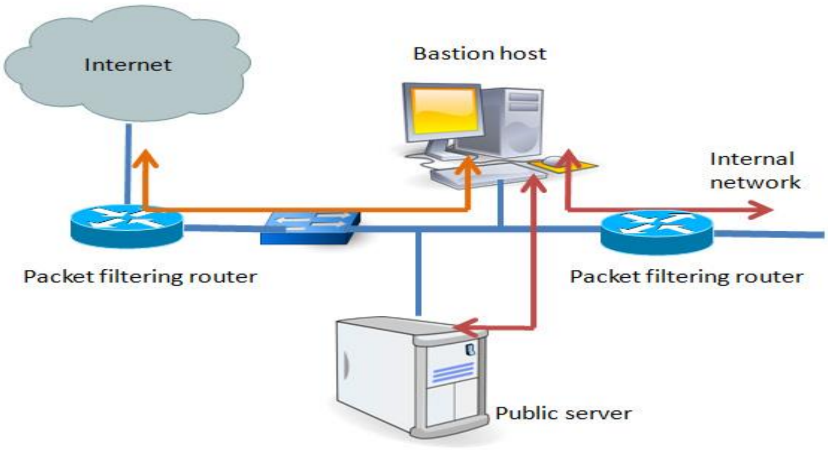
This type of configuration can have a web server placed in between the router and the bastion host in order to allow the public to access the server from the Internet. The main problem with the single homed bastion host is that if the packet filter route gets compromised then the entire network will be compromised. To eliminate this drawback, we can use the dual homed bastion host firewall system, where a bastion host has two network cards- one is used for internal connection and the second one is used for connection with the router. In this case, even if, the router got compromised, the internal network will remain unaffected since it is in the separate network zone.



Screened host firewall (Dual-homed bastion host)

2. **Screened subnet firewalls**

This is one of the most secured firewall configurations. In this configuration, two packet filtering routers are used and the bastion host is positioned in between the two routers. In a typical case, both the Internet and the internal users have access to the screened subnet, but the traffic flow between the two subnets (one is from bastion host to the internal network and the other is the sub-network between the two routers) is blocked.



Screened subnet firewall

3. **Packet filtering firewalls**

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.

Network layer firewalls define packet filtering rule sets, which provide highly efficient security mechanisms. Packet filtering is also known as static filtering. During network communication, a node transmits a packet that is filtered and matched with predefined rules and policies. Once matched, a packet is either accepted or denied.

Packet filtering checks source and destination IP addresses. If both IP addresses match, the packet is considered secure and verified. Because the sender may use different applications and programs, packet filtering also checks source and destination protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Packet filters also verify source and destination port addresses.

Some packet filters are not intelligent and unable to memorize used packets. However, other packet filters can memorize previously used packet items, such as source and destination IP addresses.

Packet filtering is usually an effective defense against attacks from computers outside a local area network (LAN). As most routing devices have integrated filtering capabilities, packet filtering is considered a standard and cost-effective means of security.

This type of firewall is the most common and easy to deploy in a small-sized network. A router functions as a firewall by examining every packet passing through the network. Based on access control list, the router either forward or drop packets. Normally, the IP address of the source and destination, port number and type of traffic are taken into account when the router processes each data packet. Since a router cannot check packet in the application layer, this type of firewall cannot defend attacks that use application layers vulnerabilities. They also fail to fight against spoofing attacks. You can use this configuration if you need higher network speed and do need limited login and authentication capacity.

4. Stateful inspection

Stateful inspection firewall works at the network layer in the OSI model. It monitors both the header and contents of the traffic. The main difference between the packet filtering and the stateful inspection is that it the later one analyses not only the packet headers but also inspects the state of the packets along with providing proxy services. Stateful inspection firewalls maintain a state table and a set of instructions to inspect each packet and store the information based on the type of traffic. It also monitors each TCP connection and remembers which ports are being used by that connection. If there is any port not required by the connection, then that port get closed.

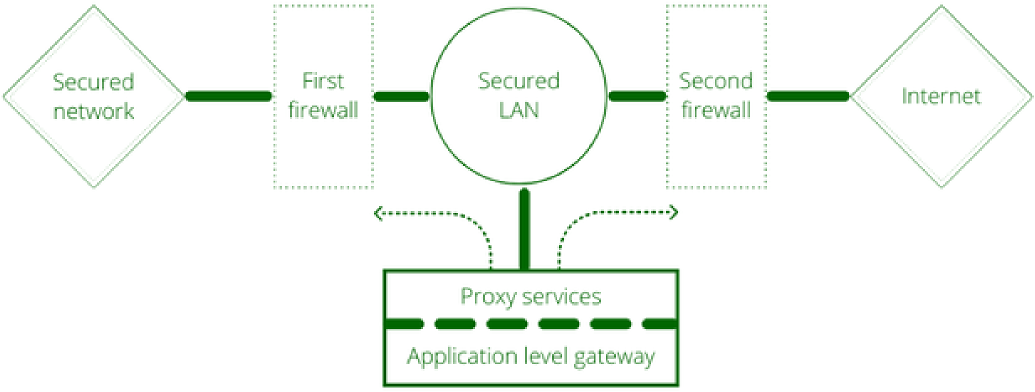
5. Hybrid firewalls

They function almost the same way the stateful inspection type firewalls work, which means they can work both in network and in application level. Normally, in a hybrid system some hosts reside inside the firewall while the others reside outside of the firewall. To communicate with the machine outside the central network IPsec tunnels are used. An example where this type of configuration is suitable is a major site connected with its branch sites via VPN. One distinct feature of this configuration is the firewall administration at the major site distribute the security policy to its branch site so as a uniform security is maintained throughout the organization.

6. **Proxy server firewalls**

Proxy allows users to run specific service (FTP, TELNET, HTTP etc.) or type of connection by enforcing authentication, filtering and logging. For specific service there will be a specific proxy. For example, if you want to allow only HTTP connection to the Internet for your internal network users, then you must allow only HTTP proxy, nothing else. Users who need to go to Internet create a virtual circuit with the proxy server and the proxy server sends the request to connect to a specific site on behalf of that particular user. Proxy server changes the IP of the request so as the Internet or the outside world can see only the IP of the proxy server. Thus, proxy server hides the internal network behind it**.** When a proxy receives the data from the Internet it sends the data back to its intended internal user via the virtual circuit. The main advantage of using proxy is that it is fully aware of the type of data it handles and can give protection to it. One disadvantage of proxy is that if there is an update of protocol that is used by the Internet, then the proxy software also needs to be updated to allow a specific service related to that protocol.

7. Application level (gateway) firewalls



Application-level gateway is also called a bastion host. It operates at the application level. Multiple application gateways can run on the same host but each gateway is a separate server with its own processes.

These firewalls, also known as application proxies, provide the most secure type of data connection because they can examine every layer of the communication, including the application data.

Example: Consider FTP service. The FTP commands like getting the file, putting the file, listing files, and positioning the process at a particular point in a directory tree. Some system admin blocks put command but permits get command, list only certain files, or prohibit changing out of a particular directory. The proxy server would simulate both sides of this protocol exchange. For example, the proxy might accept get commands and reject put commands.

It works as follows:

Step-1: User contacts the application gateway using a TCP/IP application such as HTTP.

Step-2: The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.

Step-3: After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

Difference between Packet filter & Application- level

Packet filter	**Application-level**
Simplest	Even more complex
Screens based on connection rules	Screens based on behaviour or proxies
Auditing is difficult	Activity can audit
Low impact on network performance	High impact on network performance
Network topology cannot hide	Network topology can hide from the attacker
Transparent to user	Not transparent to the user
See only addresses and service protocol type	Sees full data portion of a packet

What is a next-generation firewall?

A traditional firewall provides stateful inspection of network traffic. It allows or blocks traffic based on state, port, and protocol, and filters traffic based on administrator-defined rules.

A next-generation firewall (NGFW) does this, and so much more. In addition to access control, NGFWs can block modern threats such as advanced malware and application-layer attacks. According to Gartner's definition, a next-generation firewall must include:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention
- Application awareness and control to see and block risky apps
- Threat intelligence sources
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

Wireshark

Wireshark is a free and open-source packet analyser. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named **Ethereal**, the project was renamed Wireshark in May 2006 due to trademark issues.

Wireshark is absolutely safe to use. Government agencies, corporations, non-profits, and educational institutions use Wireshark for troubleshooting and teaching purposes. There isn't a better way to learn networking than to look at the traffic under the Wireshark microscope.

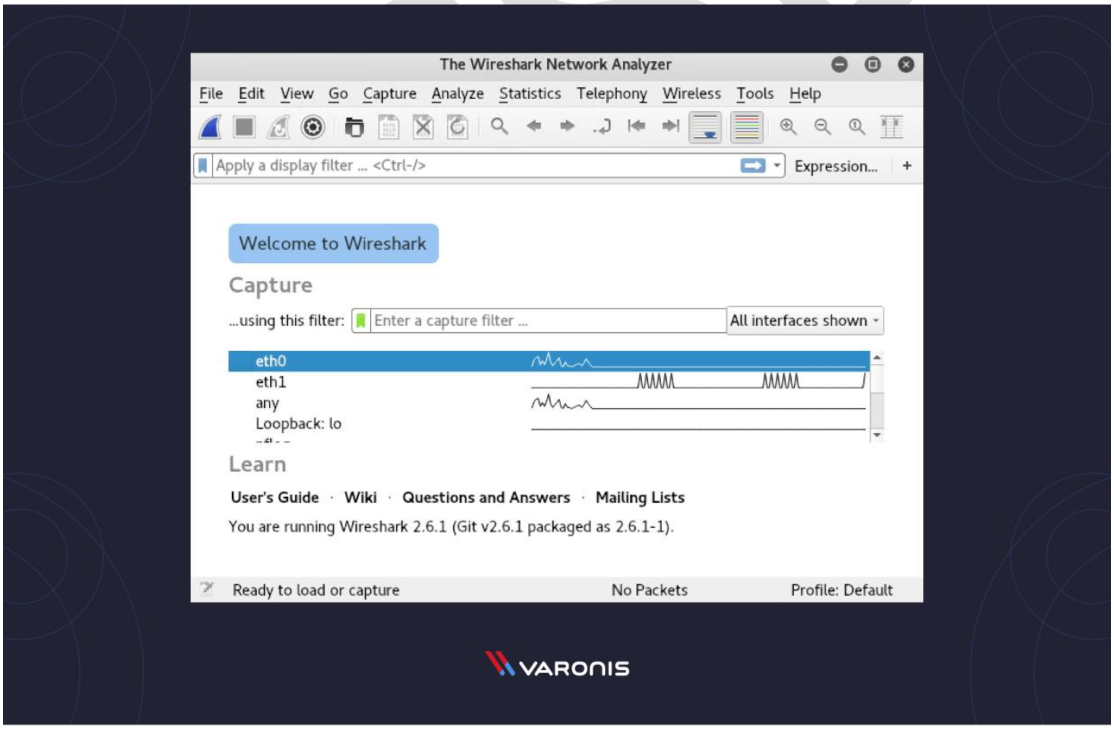
There are questions about the legality of Wireshark since it is a powerful packet sniffer. The Light side of the Force says that you should only use Wireshark on networks where you have permission to inspect network packets. Using Wireshark to look at packets without permission is a path to the Dark Side.

Wireshark is very similar to tcpdump, but has a graphical front-end and integrated sorting and filtering options.

Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyser in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic.

Capturing Data Packets on Wireshark

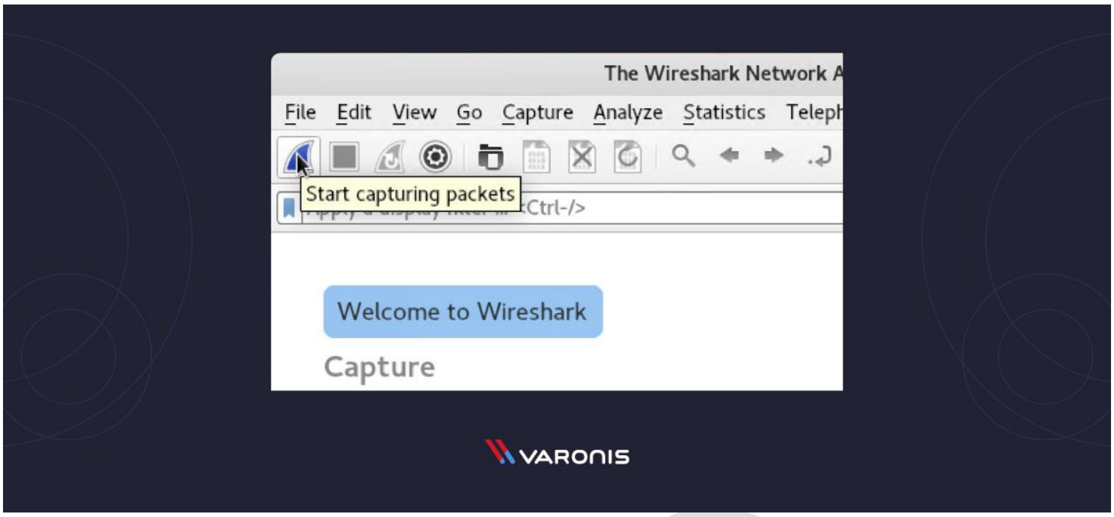
When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
eth1
any
Loopback: lo
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Default
VARONIS

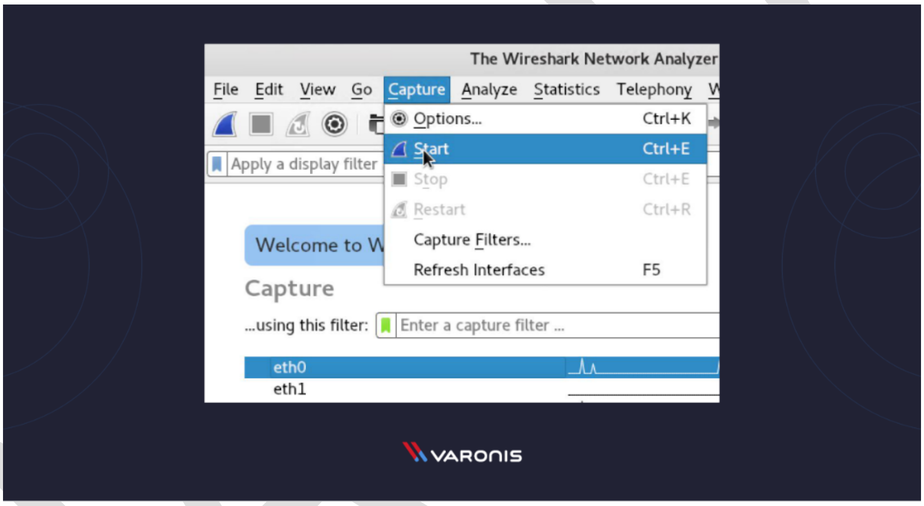
You are running Wireshark 2.6.1 (Git v2.6.1 packaged as 2.6.1-1).

You can select one or more of the network interfaces using "shift left-click." Once you have the network interface selected, you can start the capture, and there are several ways to do that.

Click the first button on the toolbar, titled "Start Capturing Packets."

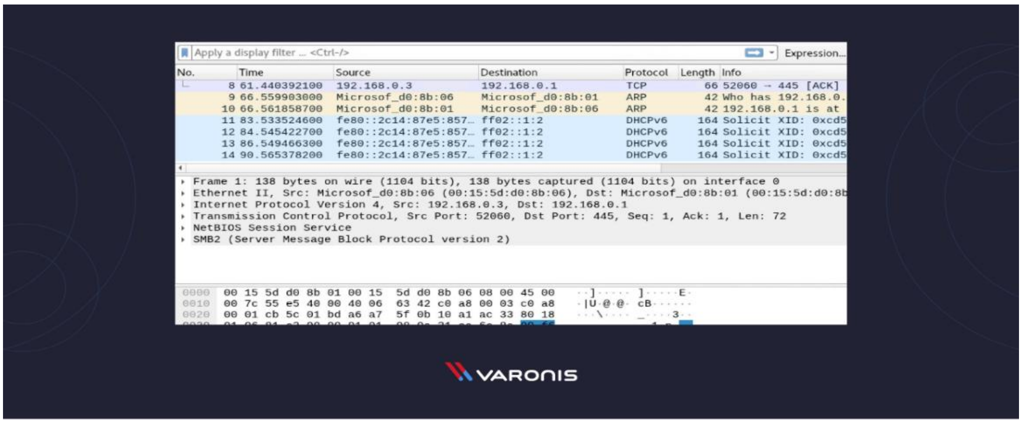


You can select the menu item Capture -> Start.



Or you could use the keystroke Control – E.

During the capture, Wireshark will show you the packets that it captures in real-time.



```
No.      Time          Source                  Destination          Protocol Length Info
      8 61.440392100  192.168.0.3             192.168.0.1          TCP         66 52060 → 445 [ACK]
      9 66.559903000  Microsof_d0:8b:06       Microsof_d0:8b:01    ARP         42 Who has 192.168.0.
     10 66.561858700  Microsof_d0:8b:01       Microsof_d0:8b:06    ARP         42 192.168.0.1 is at
     11 83.533524600  fe80::2c14:87e5:857…    ff02::1:2            DHCPv6     164 Solicit XID: 0xcd5
     12 84.545422700  fe80::2c14:87e5:857…    ff02::1:2            DHCPv6     164 Solicit XID: 0xcd5
     13 86.549466300  fe80::2c14:87e5:857…    ff02::1:2            DHCPv6     164 Solicit XID: 0xcd5
     14 90.565378200  fe80::2c14:87e5:857…    ff02::1:2            DHCPv6     164 Solicit XID: 0xcd5

▸ Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
▸ Ethernet II, Src: Microsof_d0:8b:06 (00:15:5d:d0:8b:06), Dst: Microsof_d0:8b:01 (00:15:5d:d0:8b
▸ Internet Protocol Version 4, Src: 192.168.0.3, Dst: 192.168.0.1
▸ Transmission Control Protocol, Src Port: 52060, Dst Port: 445, Seq: 1, Ack: 1, Len: 72
▸ NetBIOS Session Service
▸ SMB2 (Server Message Block Protocol version 2)

0000  00 15 5d d0 8b 01 00 15  5d d0 8b 06 08 00 45 00   ··]····· ]·····E·
0010  00 7c 55 e5 40 00 40 06  63 42 c0 a8 00 03 c0 a8   ·|U·@·@· cB······
0020  00 01 cb 5c 01 bd a6 a7  5f 0b 10 a1 ac 33 80 18   ···\···· _····3··
```

Once you have captured all the packets you need, you use the same buttons or menu options to stop the capture.

Best practice says that you should stop Wireshark packet capture before you do analysis.

Wireshark Filters

One of the best features of Wireshark is the Wireshark Capture Filters and Wireshark Display Filters. Filters allow you to view the capture the way you need to see it so you can troubleshoot the issues at hand. Here are several filters to get you started.

Wireshark Capture Filters

Capture filters limit the captured packets by the filter. Meaning if the packets don't match the filter, Wireshark won't save them. Here are some examples of capture filters:
host IP-*address*: this filter limits the capture to traffic to and from the IP address
net 192.168.0.0/24: this filter captures all traffic on the subnet.

dst host IP-*address*: capture packets sent to the specified host.
port 53: capture traffic on port 53 only.

port not 53 and not arp: capture all traffic except DNS and ARP traffic

Wireshark Display Filters

Wireshark Display Filters change the view of the capture during analysis. After you have stopped the packet capture, you use display filters to narrow down the packets in the Packet List so you can troubleshoot your issue.
The most useful (in my experience) display filter is:

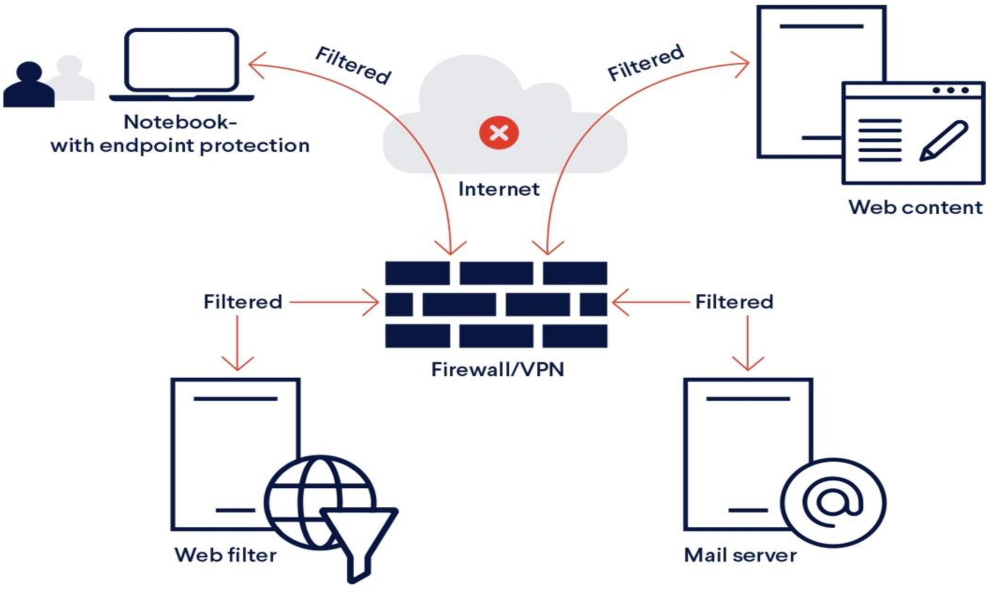
ip.src==*IP-address* and ip.dst==*IP-address*
This filter shows you packets from one computer (ip.src) to another (ip.dst). You can also use ip.addr to show you packets to and from that IP. Here are some others:

tcp.port eq 25: This filter will show you all traffic on port 25, which is usually SMTP traffic.

icmp: This filter will show you only ICMP traffic in the capture, most likely they are pings.

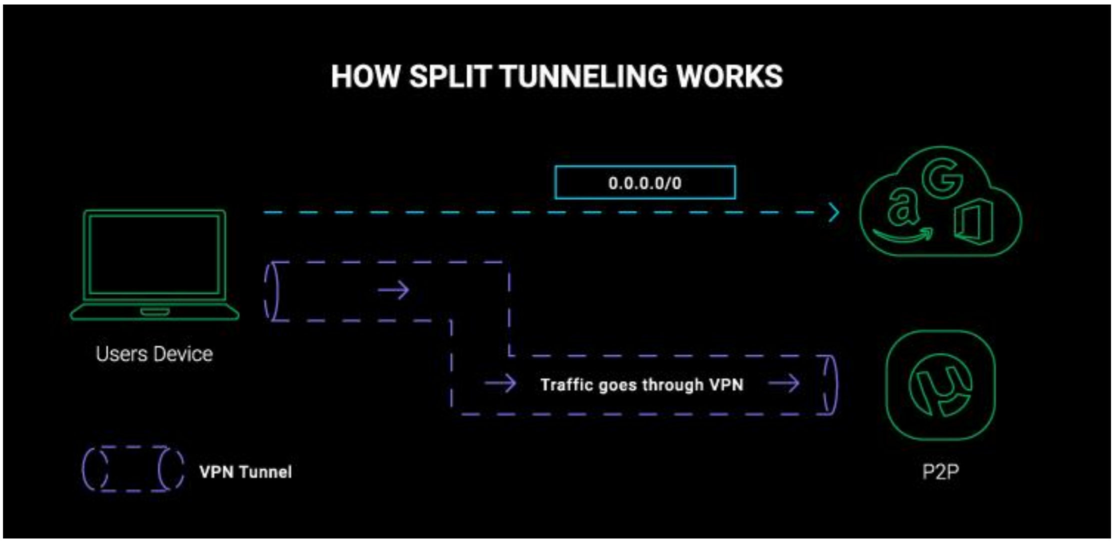
ip.addr != *IP_address*: This filter shows you all traffic except the traffic to or from the specified computer.
Analysts even build filters to detect specific attacks, like this filter to detect the Sasser worm:
ls_ads.opnum==0x09

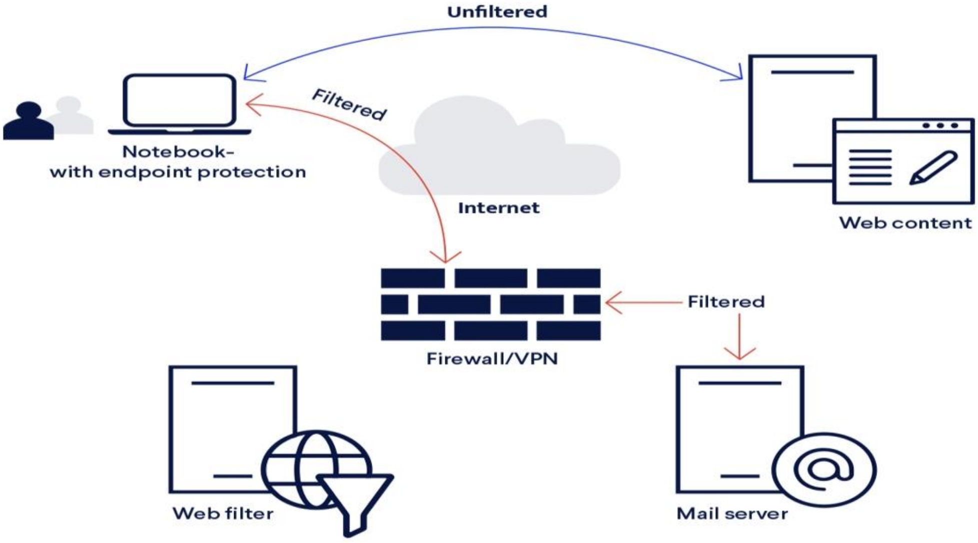
Full-tunnel VPN:



In a full-tunnel VPN scenario, whenever the user connects to the enterprise network, all network connections go through the enterprise network. Whenever the user starts a new YouTube video or Netflix movie, all network packets traverse through the enterprise network. Supporting this scenario for all employees might involve upgrading costly business Internet connection lines, network equipment, VPN servers, etc.

Split-tunnel VPN:





Split tunnelling works by giving you **two connections at the same time**: the secure VPN connection and an open connection to the internet. So, you can protect your sensitive data without slowing down your other internet activities.

Split tunnelling is a VPN feature that **divides your internet traffic** and sends some of it through an encrypted virtual private network (VPN) tunnel, but routes the rest through a separate tunnel on the open network. Typically, split tunnelling will let you choose which apps to secure and which can connect normally.

This is a useful feature when you need to keep some of your traffic private, while still **maintaining access to local network** devices.

So, you can access foreign networks and local networks at the same time. It's also great if you want to save some bandwidth.

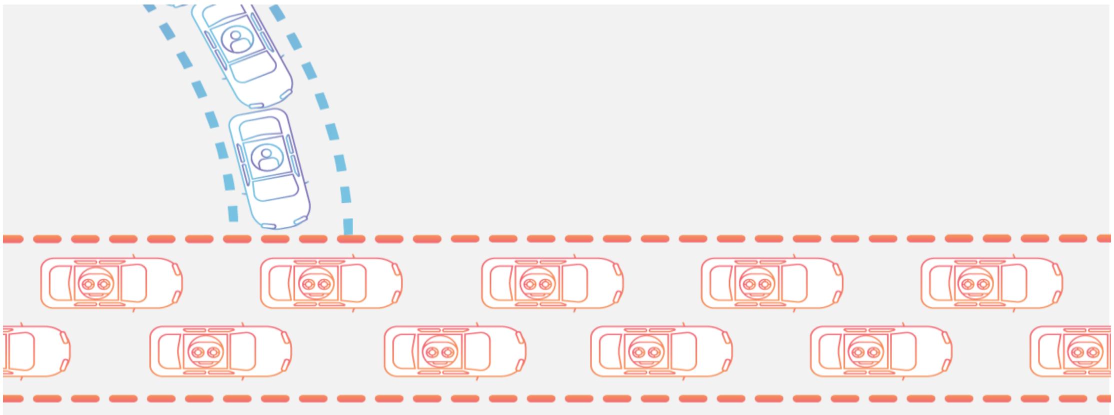
In a split-tunnel VPN scenario, only packets where the destination is in the company are routed to the company network. IT teams must set up new VPN connections for many users recently, and many IT teams choose a split tunnel. In many cases, companies had to switch from full-tunnel VPN to split tunnel due to infrastructure that is incapable of working under the extensive full-tunnel VPN load. As there is no one-size-fits-all in risk management, each company should calculate the cost difference between the full- and split-tunnel VPN scenarios, and measure this against the increased risks of malware infection, phishing attacks, etc.

Attacks-distributed

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.



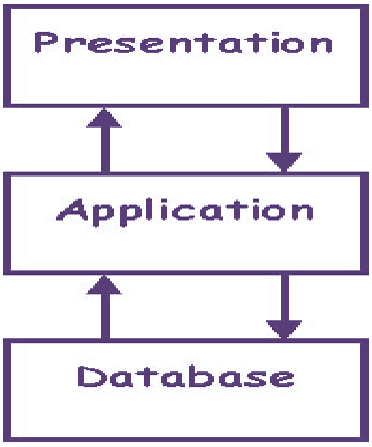
Intruder types

Intruders are the attackers who attempt to breach the security of a network. They attack the network in order to get unauthorized access. Intruders are of three types, namely, *masquerader*, *misfeasor* and *clandestine user*.

Masquerader: pretend to be someone one is not
An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account
Misfeasor: authentic user doing unauthorized actions
A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges
Clandestine user: done secretively, especially because illicit
An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

Tired Architecture

What is N-Tier? An N-Tier Application program is one that is distributed among three or more separate computers in a distributed network. The most common form of n-tier is the 3-tier Application, and it is classified into three categories. • User interface programming in the user's computer • Business logic in a more centralized computer, and • Required data in a computer that manages a database. This architecture model provides Software Developers to create Reusable application/systems with maximum flexibility. In N-tier, "N" refers to a number of tiers or layers are being used like – 2-tier, 3-tier or 4-tier, etc. It is also called "Multitier Architecture". The n-tier architecture is an industry proven software architecture model. It is suitable to support enterprise level client- server applications by providing solutions to scalability, security, fault tolerance, reusability, and maintainability. It helps developers to create flexible and reusable applications. N-Tier Architecture A diagrammatic representation of an n-tier system depicts here – presentation, application, and database layers.



These three layers can be further subdivided into different sub-layers depending on the requirements.

Some of the popular sites who have applied this architecture are

- MakeMyTrip.com
- Sales Force enterprise application
- Indian Railways – IRCTC
- Amazon.com, etc.