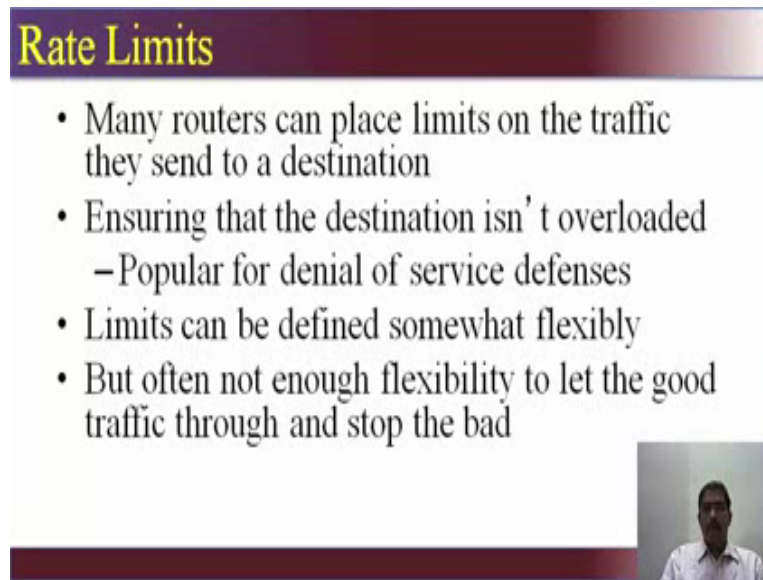


**Introduction to Information Security**  
**Prof. Dilip. Ayyar**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Madras**

**Lecture – 45**

(Refer Slide Time: 00:10)



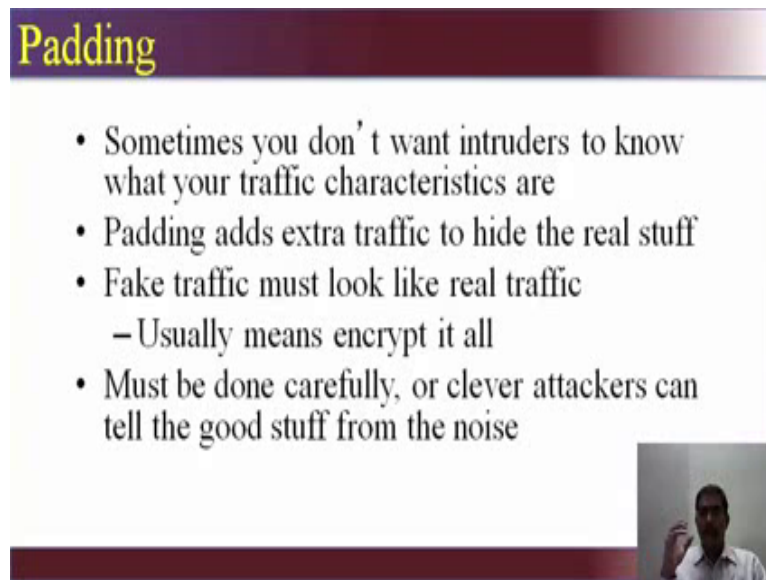
**Rate Limits**

- Many routers can place limits on the traffic they send to a destination
- Ensuring that the destination isn't overloaded
  - Popular for denial of service defenses
- Limits can be defined somewhat flexibly
- But often not enough flexibility to let the good traffic through and stop the bad

Video inset showing Prof. Dilip Ayyar

The Rate limits - many routers can place limits on the traffic that they send to the destination. It just like your ingress filtering, where you can specify that attachments over qlp cannot into those networks in the mail transmission. Similarly, you can have rate limits based on the routers. Then that ensure that destination is not overloaded that is one of the most popular methods for preventing denial of service. And limits can be defined somewhat specifically or flexibly depending upon the organization its requirements, its needs, but often not enough flexibility to let the good traffic through and stop the bad. So, you should not have so much of flexibility which is basically need that the you should have balance between what how you need to get flexible and what you need to allow and what you need to deny, so that the good traffic does not get blocked.

(Refer Slide Time: 01:18)



## Padding

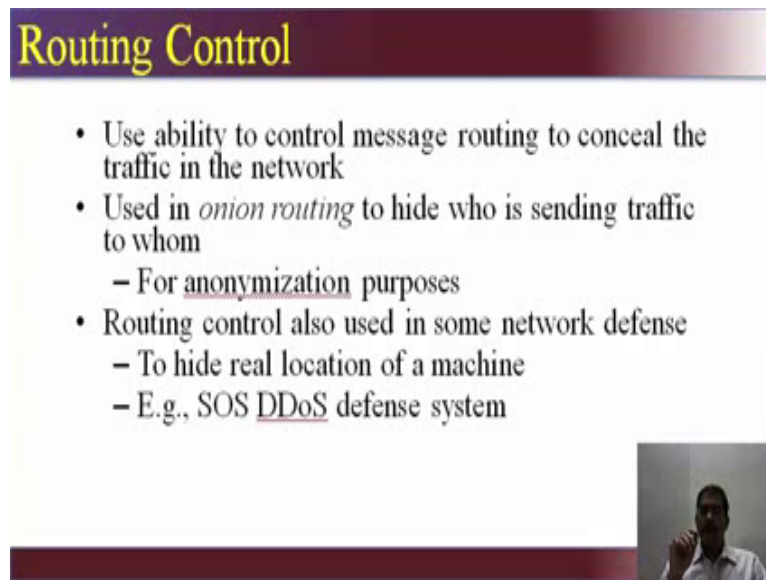
- Sometimes you don't want intruders to know what your traffic characteristics are
- Padding adds extra traffic to hide the real stuff
- Fake traffic must look like real traffic
  - Usually means encrypt it all
- Must be done carefully, or clever attackers can tell the good stuff from the noise

Video inset showing a man speaking.

We are spoken bit of traffic basically padding involves when you do not want intruders to know what traffic characteristics that are sending and receiving and padding adds extra traffic to hide the real stuff and fake traffic must look like real traffic, that is more important so that attackers should be able to analyze that this is the fake traffic and this is the real traffic ; so that means, you have to encrypt all; that means, the good traffic and bad traffic; it must be done very carefully otherwise clever attackers can tell the good stuff from noise we are getting noise into the traffic along the good traffic so that it becomes difficult for the attacker to decode what is going on in the attack.

So, what basically attackers traffic padding they produces cipher text out continuously even in the absence of plain text. A continuous random data stream is generated. When the plain text is available it is encrypted and transmitted when the input plain text is not present then random data is encrypted transmitted. So, it makes impossible for an attacker to distinguish between the true data flow or real data flow and the padded data. So, then it is also difficult for him or her to deduce the amount of traffic that is generated and it sent.

(Refer Slide Time: 02:59)



## Routing Control

- Use ability to control message routing to conceal the traffic in the network
- Used in *onion routing* to hide who is sending traffic to whom
  - For anonymization purposes
- Routing control also used in some network defense
  - To hide real location of a machine
  - E.g., SOS DDoS defense system


Video inset showing a person speaking.

That's what basically padding does. Then you continue the routing control it uses the ability to control message routing to conceal the traffic in the network it is used in onion routing to hide who is sending the traffic and to whom this is used for anonymization purposes. Routing control is also used in network defense to hide, the real location of the machine example SOS, DDOS defense system. Here the term onion routing is used. Onion routing is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several networks routes; for the onion routers it is someone building an onion. each onion routers removes a layer of interruption to unthought the routing interruption and sends the message to next router where the same process are repeated. So, this prevents the intermediatrynodes from only the region the designation that contents the messages.

(Refer Slide Time: 04:11)

## Firewalls and Perimeter Defense

- Firewalls implement a form of security called *perimeter defense*
- Protect the inside of something by defending the outside strongly
- Control the entry and exit points
- If nothing bad can get in, I'm safe, right?




So, that is what is called onion routing everybody want to know what is firewall. Firewall implements basically a form of security called perimeter defense perimeter is the area surrounding the layer bounded by surrounding the network; it protects the inside of a network by defending the outside strongly. So, it basically filters; what is allowed with the network and what should not coming to the network is stopped is basically controls the entry and exit points what can over to the network and what can come into the network.

(Refer Slide Time: 04:53)

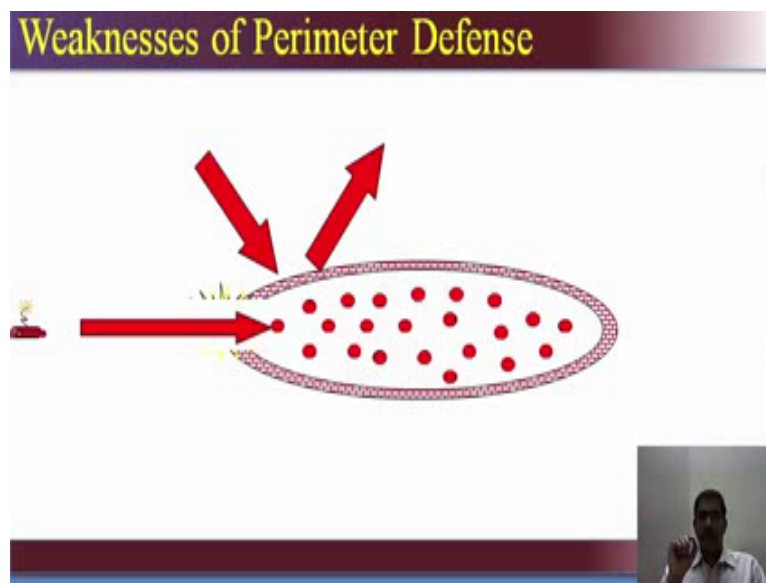
## Weaknesses of Perimeter Defense Models

- Breaching the perimeter compromises all security
- Windows passwords are a form of perimeter defense
  - If you get past the password, you can do anything
- Perimeter defense is part of the solution, not the entire solution



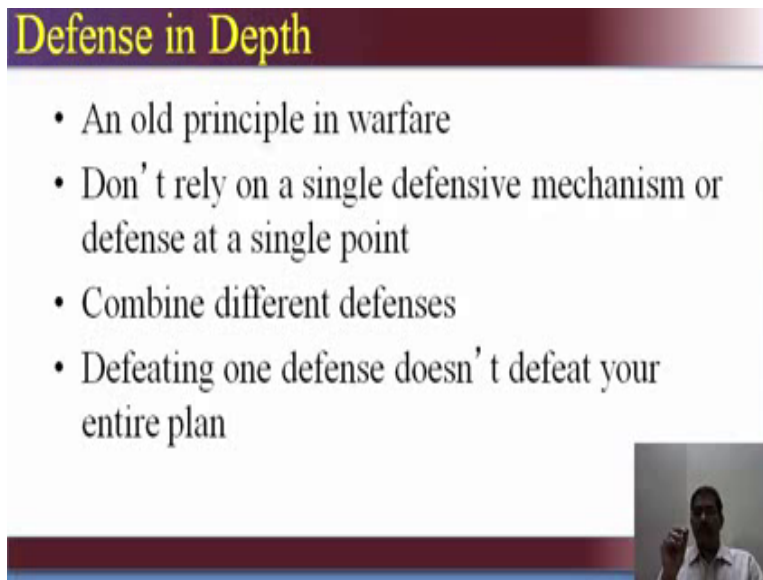
If nothing bad can get in I am safe right the general feeling there are weakness of the perimeter defense models. now what once the attackers breeches the perimeter it compromises all security, if that is the only layer of security which is available. Now windows passwords are form of perimeter defense if you get pass the password you can do anything and you take the example you cannot get inside the window password what is the administrative password or you use the password, but once you get access to the password you can login to the system then you can do anything.

(Refer Slide Time: 05:36)



So, perimeter defense is the part of the solution it is not the entire in itself. This slide indicates that precisely. Now the perimeter that there are several nodes inside the firewall coming inside and going outside attacker trying to get in to the perimeter, but if he manages to get in to the perimeter attack one over and attack can be done easily, he can can do anything.

(Refer Slide Time: 06:00)



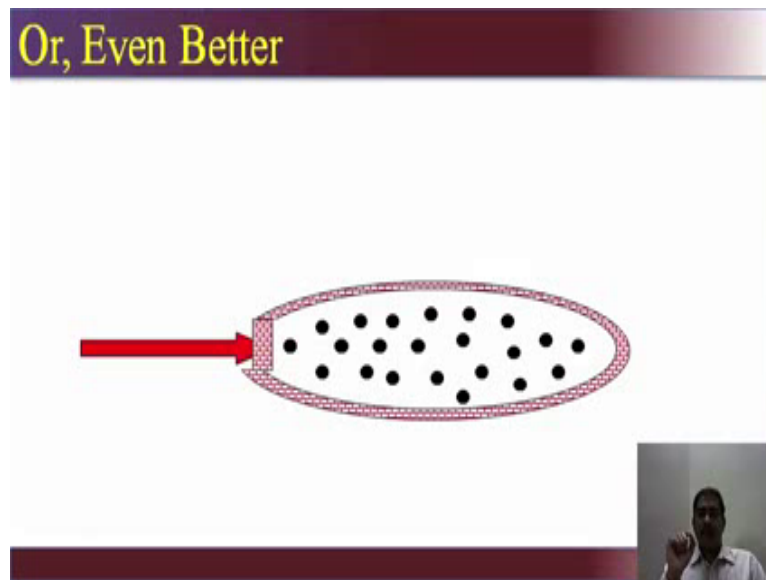
## Defense in Depth

- An old principle in warfare
- Don't rely on a single defensive mechanism or defense at a single point
- Combine different defenses
- Defeating one defense doesn't defeat your entire plan

A small video inset in the bottom right corner shows a man in a white shirt speaking.

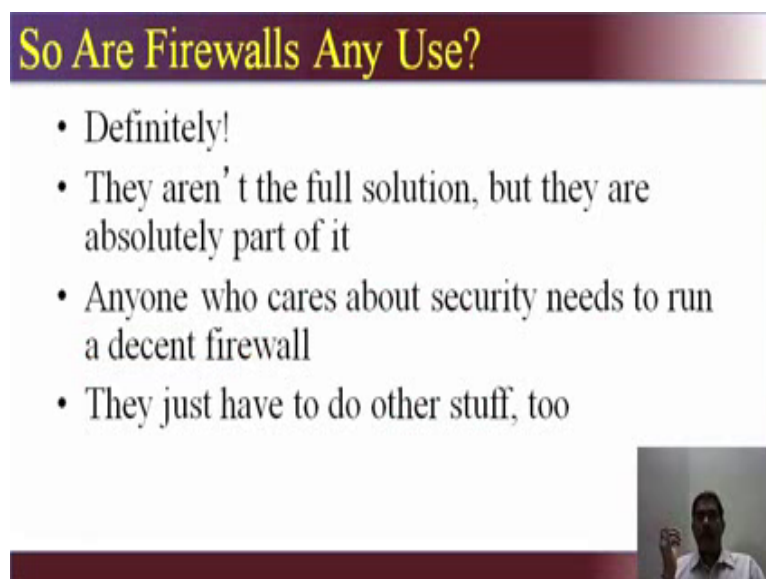
Defense, defense in depth is an old principle in warfare it does not rely on a single defensive mechanism or defense at a single point that is you should have several layers of security just like a onion routing you should have layers of security when even if you breach one layer that is some other layer protective and in the center of the onion is the core; the core of where we are someone let to get the data is core. So, you should not rely on a single defensive mechanism rather, a combination different defense mechanism it protects in some mechanism. Defeating one defense does not defeat your entire plan. So, like it you should have several layers of mechanism security where it even one layer if it breached, access to the information is entirely difficult that there are several other layers before the data can be access.

(Refer Slide Time: 07:06)



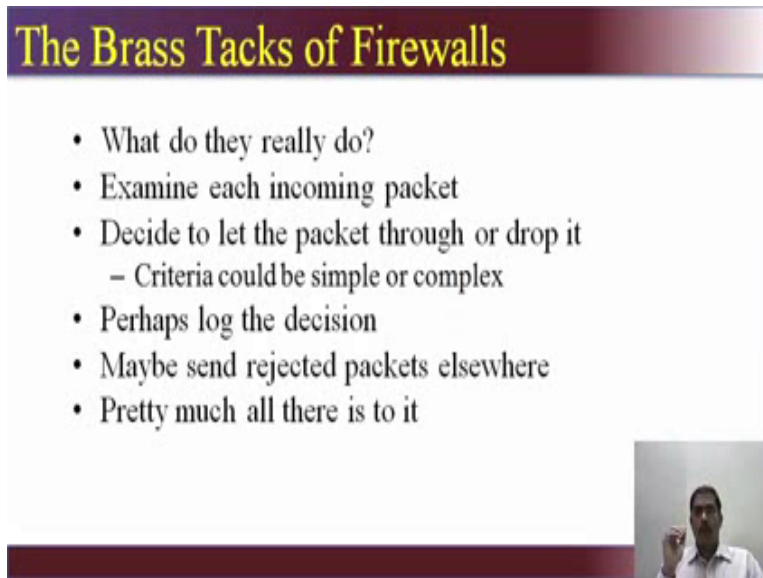
So, let say that the attackers has breached its perimeter what should happen as you can see the red dot is a compromise system; the red dot can communicate with a the black dot, another system in network and traffic can go out, so that there is only one layer of security in something within that layer is compromised, your entire network will get compromised. Now that is the another slide which says it is even better. So, you have put in another filtering mechanism so that, attackers when he tried to attack gets past the perimeter still has to encounter another level of security.

(Refer Slide Time: 07:56)



So, there the network is safe now here can see by adding another layer of security we have computer are not compromised. So, firewalls any use definitely it is use they are not the full solution, but they are a part of it or what layer of it. Anyone who cares about security needs to run a decent firewall they have to do the other stuff also now when you talk about firewall there are several popular stuff available like cisco, you have check point you have forty gate.

(Refer Slide Time: 08:34)



**The Brass Tacks of Firewalls**

- What do they really do?
- Examine each incoming packet
- Decide to let the packet through or drop it
  - Criteria could be simple or complex
- Perhaps log the decision
- Maybe send rejected packets elsewhere
- Pretty much all there is to it

Video inset showing a man speaking.

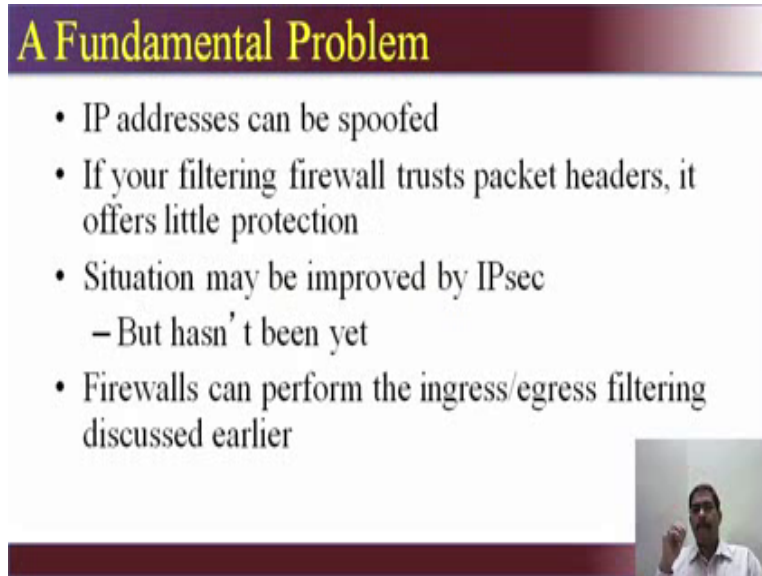
So, there are several important or the famous vendors available for your firewall. What are the basics of the firewall what do they really do they examine each incoming packet and they decide through to let the packet inside or to drop it. Now that criteria can be simple like we have explained it earlier if that source address is not in that particular range, drop it; or you can be complex and its come from particular source and it should be directed to that particular port and should have done in other characteristics it can be a complex rule also. And basically all the rules are all be filtering that happens in the firewall logged perhaps the decision to whether allows the traffic or deny the traffic is log so that a forensic be done on the firewall at a later time if required. It can also send the rejected packets elsewhere may to be different box where analysis can happen or it can be send to security incident and management tool, the SIM tool, for log analysis to see what is happening in the network.

So, basically this are the functions for the basic properties of firewall it also complex than that, but what we need to understand is it examines each packet then it decides that to allow the packet in or to drop the packet or it could send the packet somewhere else, it logs all the




traffic coming in if you configure it this criteria appropriate can be simple process or a complex process.

(Refer Slide Time: 10:25)



**A Fundamental Problem**

- IP addresses can be spoofed
- If your filtering firewall trusts packet headers, it offers little protection
- Situation may be improved by IPsec
  - But hasn't been yet
- Firewalls can perform the ingress/egress filtering discussed earlier




So, that is what basically a firewall will do. The fundamental problem is IP addresses can be spoofed; we have seen what spoofing is. So, if your firewall filtering trusts the packet headers then it offers little protection if spoofing is allowed and if your firewall relies on trusting the packet header, then it could be a problem now these situations can be improved by the implementing IP sec, but hasn't been yet many lot of people do not use IP sec for trusting or to encrypt or to filter the traffic. Firewall can performs both the in-bound and out-bound filtering, we discussed that what are ingress or egress filtering.

(Refer Slide Time: 11:14)

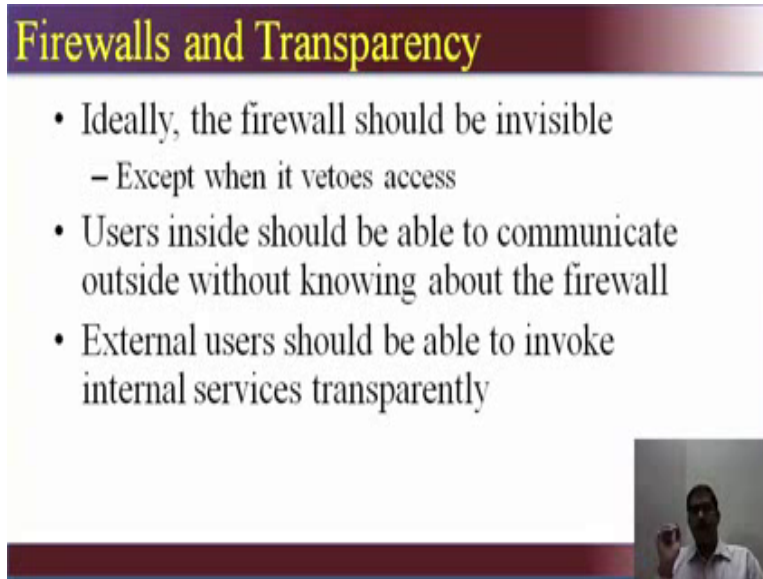
## Filtering Based on Ports

- Most incoming traffic is destined for a particular machine and port
  - Which can be derived from the IP and TCP headers
- Only let through packets to select machines at specific ports
- Makes it impossible to externally exploit flaws in little-used ports
  - If you configure the firewall right . . .



So, firewall can do both in bound filtering and out bound filtering. Again like I said it can filter based on the traffic to which port it is directed; So, most incoming traffic is destined for particular machine and port meaning it says that it can go through 10 dot 10 dot one dot one to port 80. So, it can filter based on that criteria which can be derived from the IP and TCP headers. So, it does an analysis of the IP and TCP headers. It allows packet only to select machines at select ports. So, again a firewall when you configure it, it says that from any system, to this particular server I will allow only port 443. So, it can let through packets to select machines at specific ports. So, if there are twenty servers there and the firewall rule is configured that only to 10.10.1.1 I am going to allow traffic on port 80 and not for other routers. So, it will do exactly that process, and it makes it little impossible or it makes it impossible to and externally exploit flaws in the little used ports. If you configure the firewall right. There are still these methods like ports marking and other things, it makes it impossible to exploit the flaws for the ports are not available to exploit the external attack.

(Refer Slide Time: 12:44)



### Firewalls and Transparency

- Ideally, the firewall should be invisible
  - Except when it vetoes access
- Users inside should be able to communicate outside without knowing about the firewall
- External users should be able to invoke internal services transparently

A small video inset in the bottom right corner shows a man in a white shirt speaking.

Our firewall should basically be invisible or transparent except, when it vetoes access vetoes when it except, when it denies access users inside should be able to communicate outside without knowing about the firewall means it should be seam-less. It should not be a user unfriendly experience. External users should be able to invoke internal services transparently. Now here the important thing to remember is when you talk about external users, it is external authorized users who want access into the network, not external users does not specify all external users. The external users who may have a need to do within the network.

So, with that to conclude the network security aspect. Now what we have learned in this is the basics of cryptography, what are networks what are the medias that used in communication media is used in network, what are the communication channels, what are the protocols, protocols rules of communcation, what is the basic of the firewall there are different kinds of firewall available, you can do a Google search for firewall there are different generations of firewall available. Then basically what a firewall does. now what we have not covered in this is what is a port. a port is an invisible window of a invisible channel through which your communication happens. There are 65535 ports in your computer, each one is designed for a specific purpose. 1 to 1024 are reserved for the system processes and the remaining are registered ports where a user can register or a particular vendor can register that port for a specific service.

If you take the example for different ports 21 is FTP, 22 is SSH, 23 is Telnet, 25 is SMTP, 80 is your HTTP port, 443 is your HTTPS port. Similarly, you have 110 as a POP3 port or even IMAP, 465 as your SMTPS port, or 587; So different ports, ports numbers are added there are also some frozen ports, netbios, subseven, users ports in the range of 6000 series or 60000 also, then you have 3389 is your RDP services; so there are different kinds of ports for different; your database ports there are Microsoft SQL uses ports 1433 your my SQL uses 3306, your oracle uses 1521 to 1526. So, there are different services available on different ports. Now again going in to details of course you will get what each port is designed for what by Google-ing. So, there is an agency for IANA which has the entire list or it is a port registered authority where you get the list of all port numbers and transport control ports. It's a transport protocol port registry. So, you will get more information in that. After ports there are IDS IPS which is intrusion detection system intrusion prevention system. So, IDS basically checks the traffic for malicious activity based on criteria, on certain database. IPS is prevention system. Then you have anti-spam, email filtering. So, there are several aspects when it comes to network security. In the next session, we will go in to what is vulnerability assessment, what is penetration testing, how do you basically understand the phases of this VA or VP, what are the general or popular tools available for conducting the vapt.