

**Internet Technology**  
**Prof. Indranil Sengupta**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**  
**Lecture No #31**  
**Internet Extranet and Firewall**

From today's lecture, we shall be starting some discussions on security issues in computer networks. Actually we shall be talking about a few things. First we shall look at some of the security infrastructures that we require. Then we shall look at some of the low level techniques and technologies that we need to know about. Then we shall tell look at some of the typical applications that have been devised to work on the internet to make transactions safe and secure.

(Refer Slide Time: 01:32)



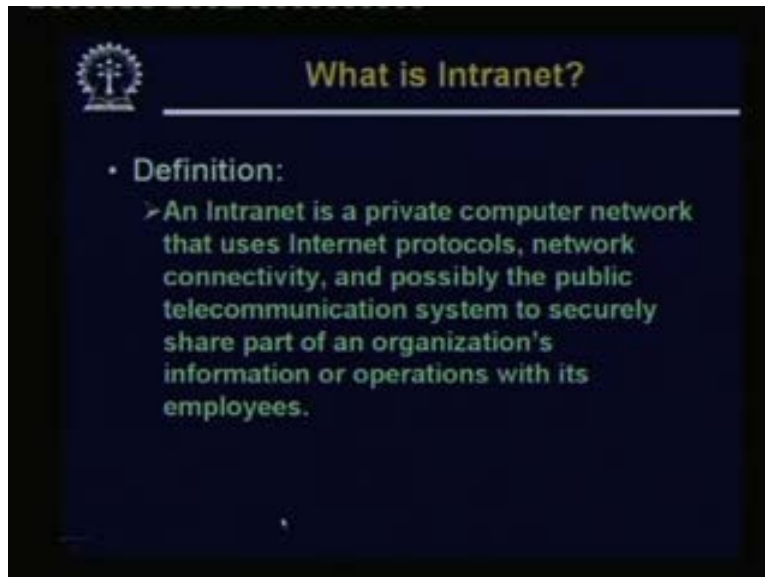
The first lecture of the series is titled intranet extranet firewall. So we shall be looking into these three different kinds of things in some detail today.

(Refer Slide Time: 01:47)



Let us first try to understand what is the meaning of the terms in intranet and extranet and how do they differ?

(Refer Slide Time: 01:59)

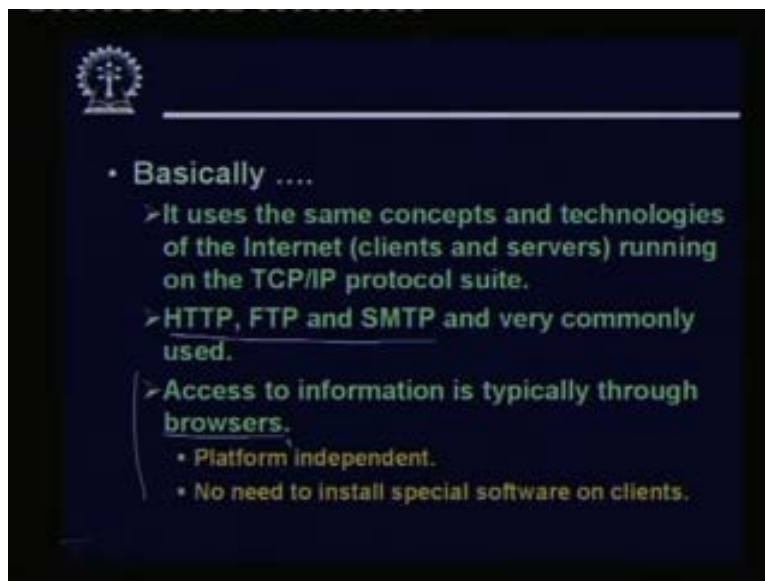


Let us start with the definition of intranet. As many people accept intranet as per its definition, it says it is a private computer network. So this is important that an internet is a private computer network which means it is owned by a particular company or an organization. This is important here. So internet is the private computer network that uses internet protocols network connectivity and possibly the public telecommunication system. Because if the organization is large then possibly for communication they are

also using the telephone lines to securely share part of an organization's information or operations with its employees. This is definition, what it actually means? It means suppose we have a company, we have an organization; we have a number of employees. Employees are of several different types; there can be managers there can be supervisors there can be clerks and other engineers. What we are saying is that the company's information system would be maintaining locally in some server inside the company and all the employees will have access to the information system over the network.

If you are using internet technology or if these applications are based on internet protocols, and then possibly you can use this simple browser on your machine to have access to whatever information you want. Secondly there can be other security issues built into the system so that I am a manager; I should be able to see everything I want. If you are an engineer you should only be allowed to see your viewer modify the segment of formation that you are allowed you are allowed to access. So intranet means this you use internet technologies TCP/IP develop application using the tools and technologies which people have been using over the internet. Advantage is that you can use this standard user interfaces applications like the browser to access the system. And this is called intranet because this is only internal to your company. Outside users are not allowed to access or have access to this kind of a service. Typically this is behind a firewall so that outsiders cannot access.

(Refer Slide Time: 04:44)



So as I said it uses the same concept and technologies of the internet. This is also based on the client server technology. They are running on the TCP/IP protocol suite and some of the very commonly used applications are as I said TCP, FTP and SMTP. So these are the very typical applications which are there and as I said users typically use the browser s at the front end only. They do not keep any other application programs to be loaded on the machines. This makes using the system platform independent. There is no need to install any special software.

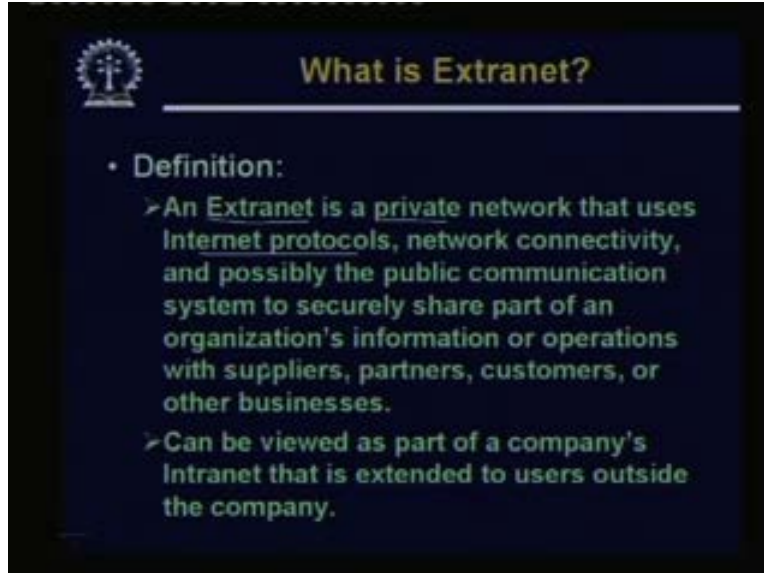
(Refer Slide Time: 05:29)



Advantages are obvious, such a system will help employees to quickly locate and access information and the applications which are relevant to their usages. Depending on the segment of the employee the information you are able to view the kind of applications. You are able to run that will be different and since interface is based on browsers, this will allow you so called access from anywhere. Sitting anywhere you can have access to this. Such intranets can serve as a powerful tool for communication. Both vertically and horizontally means you can have a means for communicating and co.

And you can say cooperating with your co-workers at the same level in the higher or there can be some kind of a communication mechanism between your superiors. And your superiors can give your directive. So the same infrastructure can be used to provide all this kind of communication. Suppose you are working in a group in a team towards development of a certain product. So all the workers in the group can share information can discuss, can get to know the details of what the other members of the team is working on. If they have a suitable such intranet to working place. So this also permits information to be published so that other employees can view them.

(Refer Slide Time: 07:12)

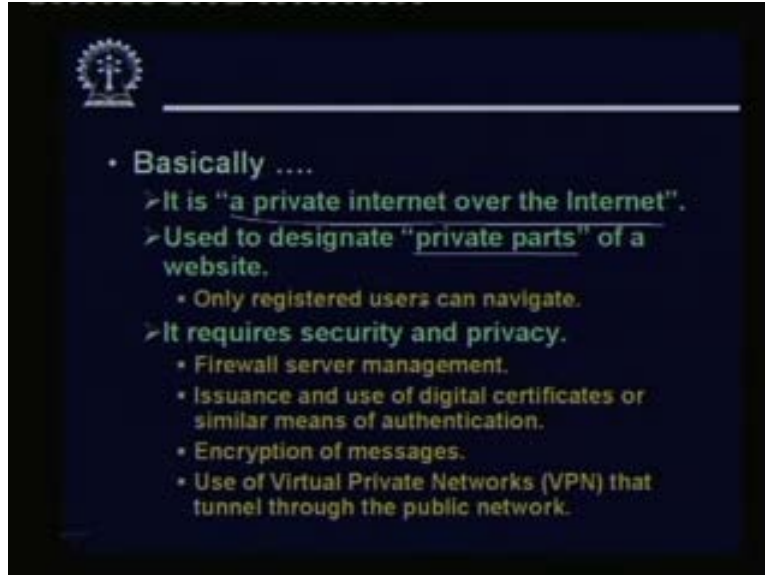


See extranet is the other terminologies which people use the conceptually extranet and intranets are similar. There is one major difference. Extranet is also a private network that also uses internet protocols network connectivity public communication system everything but the difference is that this extranet is not only limited to the organizations employees. Extranet can be accessed by some outside agencies also like suppliers who supply some equipment on good store company partners. There can be business partners, customers; you may like to provide some service to the customers or some other businesses.

So basically extranet says that will I have intranet. This is something which helps me solve my internal organizational problem and the way we communicate. Now suppose we are service Provider Company. We would like a very you can say flexible link with our customers. So that the customers can continuously get updates on what is happening. If they face any problem they can send the request to us. Some persons from our organization can be responding back with the solutions to the queries and so on. So this is like having an intranet with some designate outside users also been allowed to use our access.

Obviously security will be an issue here because how do I know that other than the authorized customer, some other persons are also trying to enter our system. So there should be good authentication and you can say encryption, decryption mechanism placed to use such a system. So essentially an extranet, you can say this is like a company's intranet which you have extended to some users outside the company; not to everybody but to some selected users.

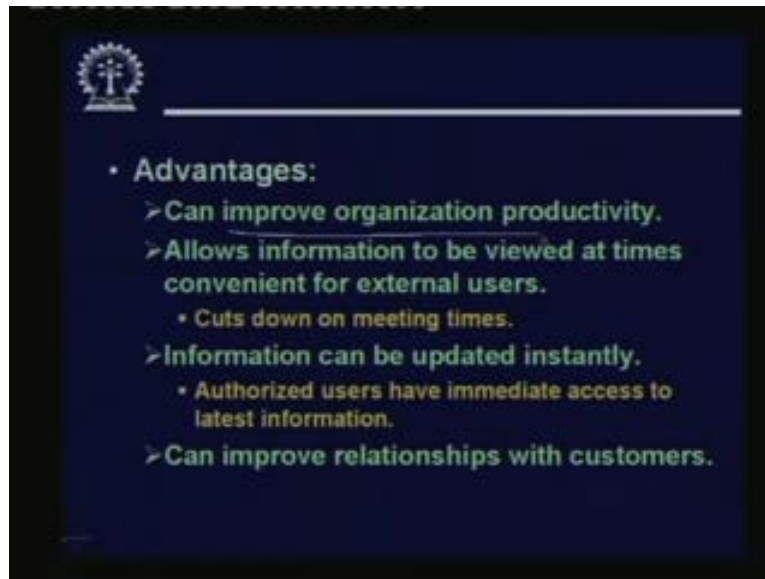
(Refer Slide Time: 09:30)



So it is basically a private internet over the public internet. So you can identify that which parts you want to make private where only the registered users can navigate. You think of some sites which are very popular. Now days there are many websites who offer some kind of online courses. They provide you online lecture notes materials. They conduct online examinations but only persons who have registered for that course will be allowed to view or access those information's. So this is also an example of an extranet. As I said for an extranet security and privacy is a very important issue and it plays a very big role. You need to very carefully manage your firewall servers so that unauthorized users should not be able to enter your system. Some very powerful and safe authentication mechanism is required so that you can authenticate or verify who is trying to use our system.

So you can use something called digital certificates which are pretty well known over the internet. For this purpose, some confidential information you may want to send over the network. You need to encrypt some messages and there is some technology which is already there like virtual private networks or VPNs where basically you are defining some kind of a private network on a public network. And when you have a VPN, these encryption-decryption mechanisms are automatically done. So any communication over the VPN will be encrypted. So even if a third party tries to listen what is going on that fellow, will not be able to understand anything. Because all communication will be hidden or will be encrypted in a form that cannot be easily understandable by a third party.

(Refer Slide Time: 11:42)



So advantages of course it can improve our organization productivity. Because if you can also include the customers and the other relevant parties to share your information. The main point is that here you are allowing information to be viewed at times which are convenient for the external users. Like otherwise what would I do, I otherwise one of our engineers would be visiting the customer sites. Or you may ask the customer to come to your company and have a meeting with the persons out there. So that we can basically coordinate the activities but here the customers know that I have a mechanism of getting some information whenever I want.

So I can do my homework well, so that before I actually have a meeting I know exactly what we are expected to talk about, that is one thing. And of course it can also help in cutting down the number of times and the duration of the meetings. And since the information will typically be updated instantly and continuously so authorized users will always come to know about these. This obviously will improve relationship with the customers because the customer can now feel that there is much better transparency in the operation of the business house. They can know exactly what is going on, I can send my request, I, get back my response from immediately. So these are something which improves in you, can say development of a good and long term relationship between the business house and the customers.

(Refer Slide Time: 13:26)



Now let us come to the issue of firewall. Firewall again is a generic term. Both in intranet and extranet we require firewalls. Firewall essentially is the mechanism using which we can filter out unwanted access attempts to our servers and networks. We want to protect our network from external intruders. Firewall aims to do exactly that, so let us see what are the objectives of a firewall and how do we do it.

(Refer Slide Time: 14:07)

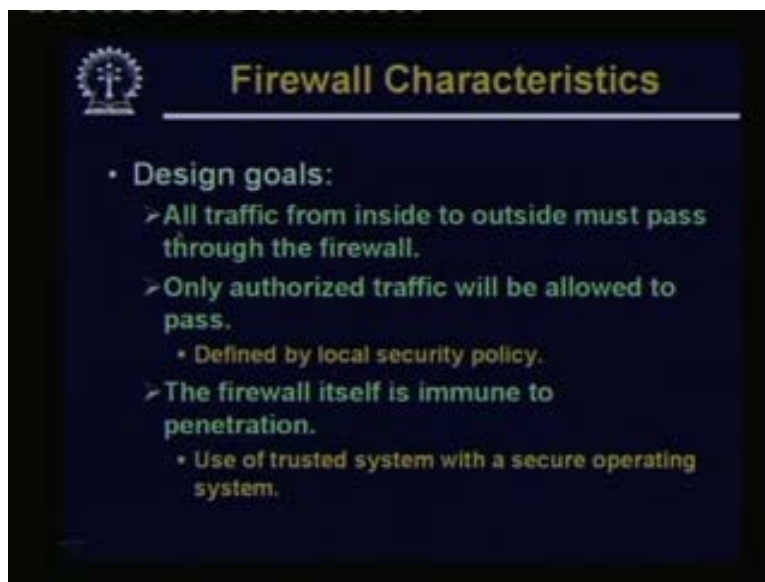


Firewalls we use to primarily locate to protect our internal network to protect the local systems which are there as part of our own network. Protect against several network based security threats. There are so many published kinds of security breaches and threats



which are possible today. A firewall tries to protect our network against these. It can also provide internal users to have a secured and controlled access to the internet and it can also provide restricted and controlled access from the internet to the local servers. See everything inside your internal network should not be hidden from the outside the world. There are certain things or certain servers you do want that outsiders should be able to have access to. Like you can think of your web server, your mail server where someone else from outside wants to send a mail, so the packet has to reach your mail server. So these are two examples I have sited. These are some servers which need to be directly accessible from the outside world. So you need to have some kind of restricted access to this kind of servers for meaningful operation of the systems.

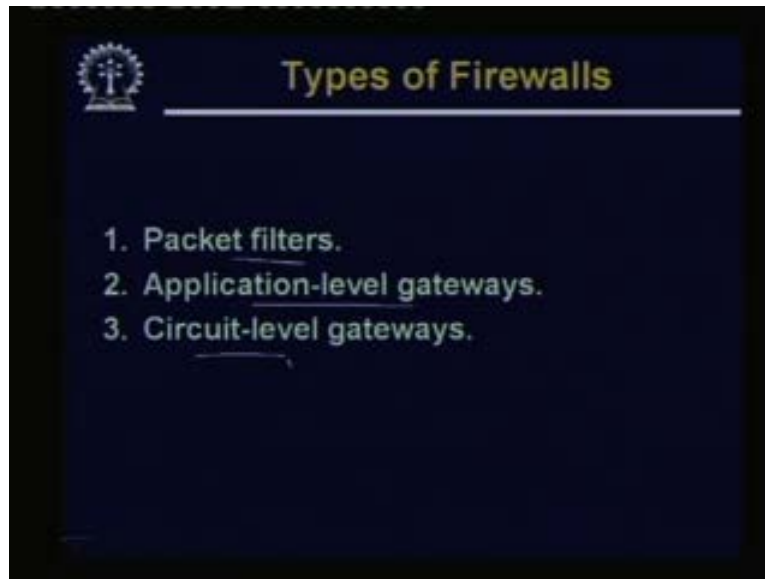
(Refer Slide Time: 15:40)



Some of the firewall characteristics in terms of the design goals are that sees the first point is very important. That all traffic flowing from inside to outside of course it is more general also from outside to inside must pass through the firewall. Because if you say that some of the data package will flow through the firewall and some will not. Then the packages which are not forcing to be flowed through the firewall they may be caring with them some malicious content or some threat. So in order to protect best from external threats you must ensure that everything flows your firewall. So you can define some so called local security policy or rules using which you can specify that what to mean by authorized traffic.

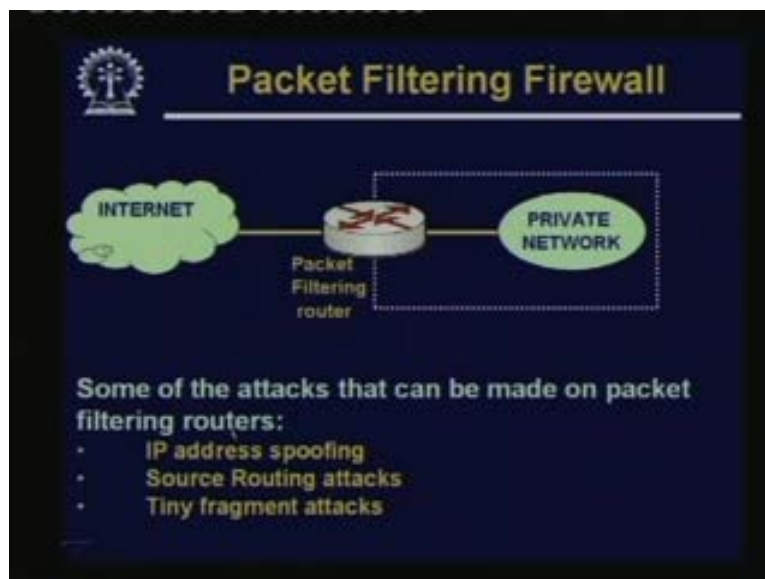
Only such authorized traffic will be allowed to pass and of course the firewall system itself should be very carefully designed. Because you should not have a situation where someone can easily break into the firewall and start tampering it. So the firewall system itself it is also nothing but a computer. So that should be a very special kind of a computer which is not very easy to break into right. So we will see there is a concept of a trusted system secure operating system. All this things you can use to make a firewall more robust.

(Refer Slide Time: 17:28)



Broadly speaking there are three types of firewalls we encounter. Firewalls based on packet filtering mechanism. Based on application level gateways, based on circuit level gateways, let us try to see what these are.

(Refer Slide Time: 17:54)



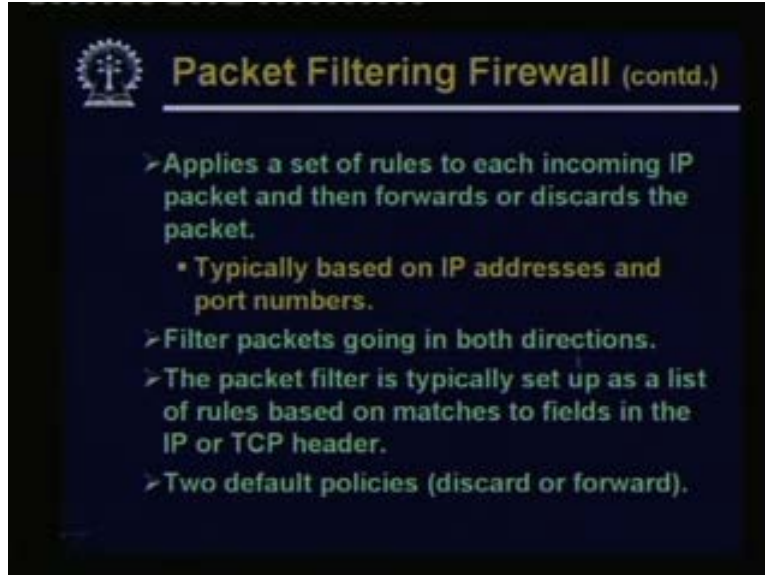
First let us look like look at the simplest of the lot the packet filtering firewall. Now you see in many such filtering environments our main objective will be to filter some packets and the first place that we look at to take decisions regarding filtering are the packet headers themselves like I am giving an example. Suppose I want I want to enforce a rule

that no one should be able to do a telnet on my machine whose IP address is this xyz. So I can specify a rule that all packets whose destination address is xyz and whose port number is 23 should be blocked. So in this way rules based on your IP address, based on port numbers can be specified and rules can be two types; either access rules or deny rules.

You can say that this communication you always block or this communication you always allow. So there are two kinds of rules you can define. So a packet filtering firewall tries to do exactly this and the architecture typically looks like this. Here we are basically using a conventional router to carry out the packet filter. Filtering operation we do not have any explicit or separate equipment which we are using at the firewall. Normally the routers which we use they are actually we can have a configuration mechanism where we can specify that what are the kinds of packets you can drop? What are the kinds of packets you can allow? So just by manipulating the table itself we can make a router work as a packet filtering firewall. So on one side we have our internal private network to which this router is a part and the internet connection is made through the router on the other side.

So we can just put in some rules in this router which will be able to filter some of the packets. Now this method is not very secure in the sense that some kinds of attacks which are well documented, that are possible to be mounted on this kind of a system like IP address spoofing. Someone can change the IP address, so all rules based on IP addresses will fail source routing attacks. These are also some attacks which can be made to the system and some there is another attack called tiny fragment attack which is also possible. So mount on this kind of system, so I am not going with detail of these attacks. But idea is that there are attacks which can be mounted on the systems and which can be mounted rather easily. They are pretty, well documented and they are websites which clearly explain how such attacks can be mounted on a network.

(Refer Slide Time: 22:17)



**Packet Filtering Firewall (contd.)**

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet.
  - Typically based on IP addresses and port numbers.
- Filter packets going in both directions.
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
- Two default policies (discard or forward).

So as I said in this method we are applying a set of rules to each incoming packets which enters the router and depending on the rule we either forward it or discard it as is said. These rules are typically based on IP addresses and port numbers. In general there can also be based on some other field of the IP address and in general such a filter can filter packets going in both directions from internet to the outside or the reverse. And the packet filters capability is defined by this set of rules or the set of rules is typically stored in a table. And as I said depending on the combination you are giving you can specify the rule to discard a packet or forward a packet. These are the two possibilities.

(Refer Slide Time: 22:25)

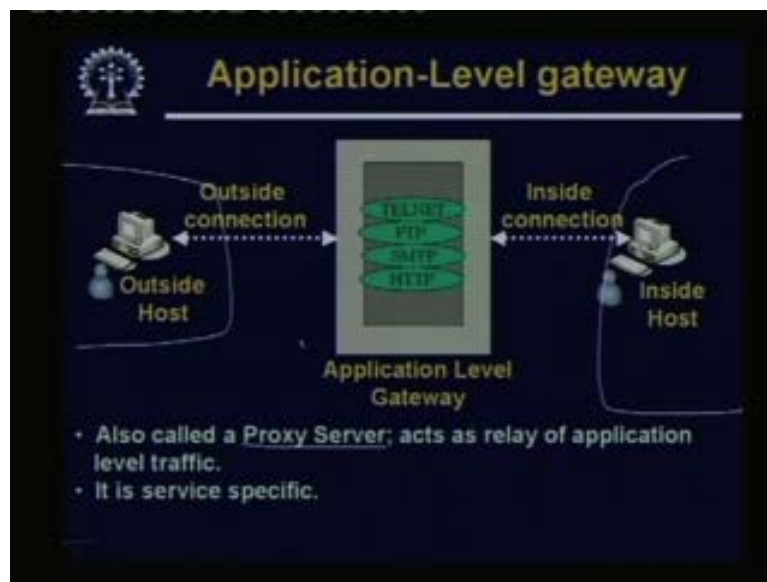


**Packet Filtering Firewall (contd.)**

- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of authentication

The advantage of this kind of firewall is that, it is very simple you need not invest separately any equipment. Transparency to the user is the users need not know about the presence of the firewall and this is also typically high speed. Disadvantage is that for a very general situation it may be difficult to set up the packet filter in rules. Because in general organization you can have a large number of combinations of IP addresses port numbers related to what they are allowed to do, what they are not allowed to do. Actually this can boil down to a very large number of rules which you need to put up in the router table. And larger the table more time it will take to search it and decide with the two forward or block a package right. And the second thing is that lack of authentication we are not using any cryptographic technique here anywhere. So that here attacks like IP spoofing can be carried out where someone can change the IP address of a network of the machine and can gain some get some unwanted advantage or authorization which otherwise that person is not allowed to have.

(Refer Slide Time: 23:47)



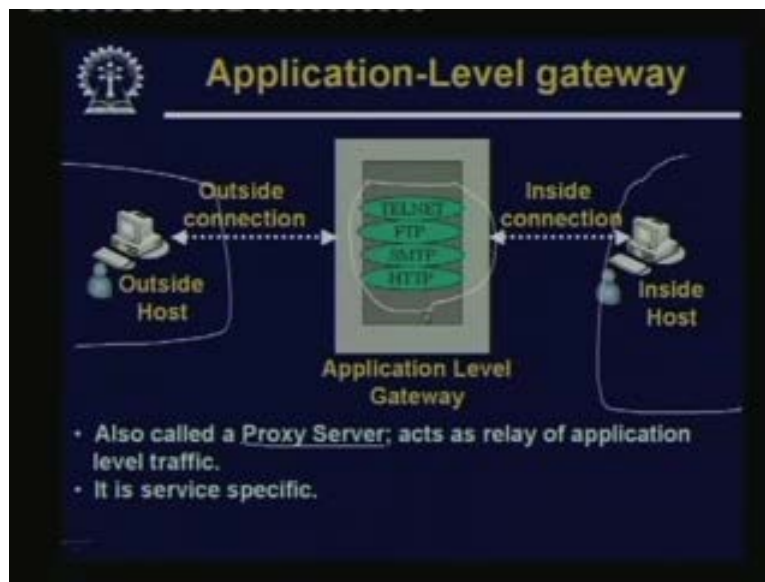
Now, the second kind of firewall. This is called an application level gateway this is more commonly called a proxy server. But typically this application level gateway is not a dedicated box like a router. This is typically a computer, this application level gateway or the proxy server sits between your internal network and the outside internet. Now the idea is this, a proxy server is service specific. Let me tell you in our network, in our institute network we use proxy servers and whenever we access the internet in the browser there is a mechanism for setting which proxy server we want to use or means and over which port number.

So the IP address of the proxy number proxy server and the port number on which the proxy server is receiving the request must be set explicitly by the user in the browser. Which means the presence of this kind of application level gateway is not transparent to the user users know that there is a proxy server existing. So once I set this proxy server address whatever request I make all my request will flow through the proxy server. And

in the proxy server there can be several set of rules I can specify. I can say that these are the sites I would not be allowed to access. These are the contents, if the contents of the request are the URL contents some specific strings I should not be allowed to pass those requests or means I can also specify some very generic rules.

Like I would not like any one to send a request to download a video like mpeg or AVI file. I will not allow in terms of the file extension I can specify. These are some examples with respect to web http. Similarly I can have some rules set up with respect to mail, email. For every email which is receiving or going out I can do a virus checking. I can filter emails based on contents some objectionable contents if I find I will drop that email with a message to the sender. So these are very service specific filtering rules we can have here. So this kind of application level gateway as is shown here, there can be several services you can think of.

(Refer Slide Time: 26:49)



And these rules are the techniques which you are filtering will be very much service specific. This basically acts as a relay of application level traffic and it is service specific.

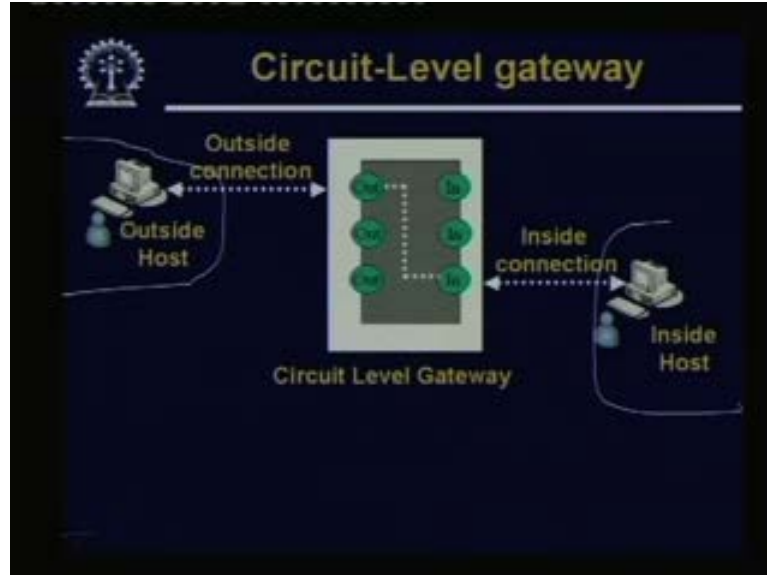
(Refer Slide Time: 27:06)



As said this is more commonly known as a proxy server. Essentially these are relay of application level traffic advantage is that; this can provide you higher security and flexibility than packet filters with respect to the way you can specify the filtering rules. Now here since you are specifying the rules which are application specific the rules; can be much more meaningful just not always only based on the IP addresses and port numbers. Also based on the contents of the packets. I can have some rules and here depending on the kind of applications you want to filter you need to scrutinize, only those applications and also it is easy to maintain a log like.

Now you know that which person in your organization is doing what kind of activity. Because all his activities are flowing through the proxy server and the proxy server is maintaining that information in a log file. So this also sometimes becomes helpful if you want to trace back some event to. Say the origin of the event why it occurred, so the log helps in doing that. Disadvantage is that you need to make additional processing on each connection due to the presence of the proxy servers. Secondly since proxy servers are computers, they are typically much lower as compared to routers where there is lot of acceleration which is done based on hardware devices. So these are some of the disadvantages.

(Refer Slide Time: 28:53)

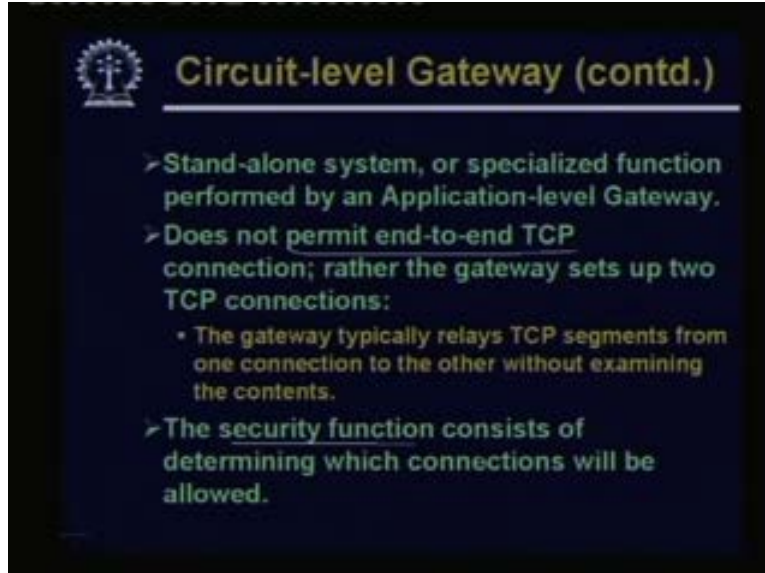


The third type is something called a circuit level gateway. This is something like this more like a tunneling like from the inside. I have a host out here. I want to access some service in some outside host or the reverse. The host from the outside wants to access service inside. So I establish some kind of a tunneling connection and after establishing a connection what happens is that whatever I sent they will be encapsulated and sends over the tunnel to the other side. So the contents will not be decoded. So this is called circuit level gateway as if I have established a circuit and once I have established a circuit I can send whatever, that will be straightaway flown to the other side over the circuit. Let me give an example of where this kind of tunneling is used. You see normally inside a land or inside a network we use the mac addresses internet addresses and the IP addresses.

There are specific technologies there. So there we talk about IP packets we talk about TCP and UDP packets and so on. But suppose I have a least line link from my organization to the office of a service provided that link may be some other link which uses some other protocol like the x.25, that is a void area network protocol which does not understand TCP or IP. So now what I will have to do. I will have to take the IP packet I will have to hide that IP packet inside that x.25 header and send the whole thing as an x.25 through tunneling. So my whole packet reaches the other side after taking out the x.25 header, I get back the original IP packet. So now in the other network I can now again process that IP packet to a site where next to forward it. These are examples of tunneling and the circuit level gateway tries to do exactly that it tries to send some information directly over an already pre established connection without processing any content.



(Refer Slide Time: 31:24)

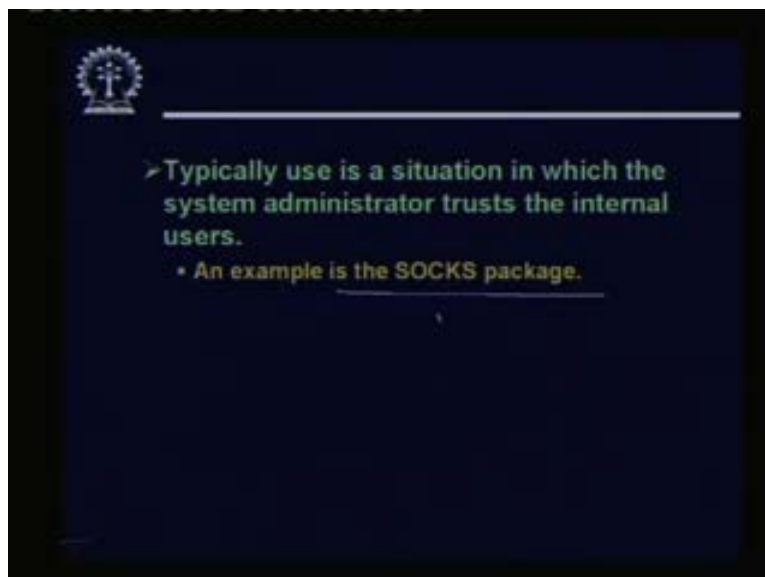


**Circuit-level Gateway (contd.)**

- Stand-alone system, or specialized function performed by an Application-level Gateway.
- Does not permit end-to-end TCP connection; rather the gateway sets up two TCP connections:
  - The gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.

So these are typical specialize as I told you of the application. This does not usually permit end to end TCP connections; only IP packets can be forwarded. Rather the gateway will set up to separate TCP connection, say gateway to the internal node gateway to the gateway to the external node. There will be two separate TCP connections maintained and the gateway will be carrying out some transmission of this TCP connection within. So here this security or the filtering rule should specify that what connections will allow and what will not allow.

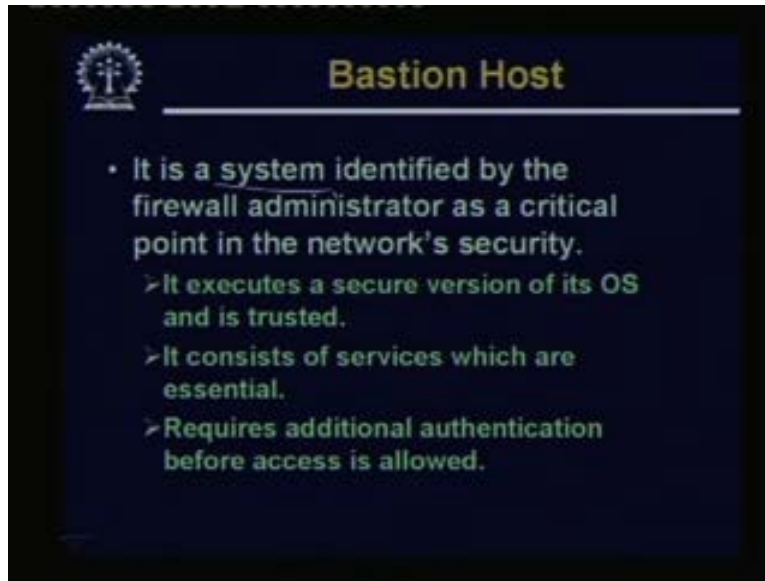
(Refer Slide Time: 32:11)



- Typically use is a situation in which the system administrator trusts the internal users.
  - An example is the SOCKS package.

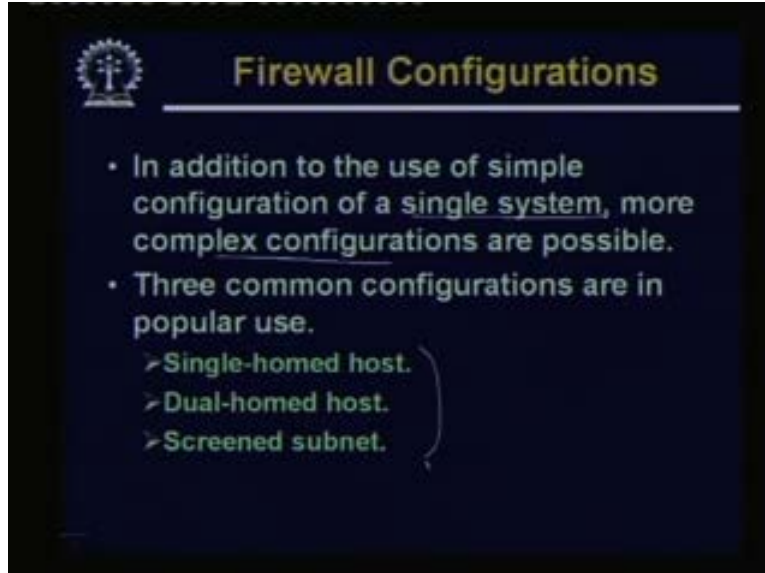
One example in the security related situation that this kind of filter is used it is socks package which many of us use for secure transmission. This is just an example. Now we come to something called a bastion host. Bastion host this term comes in connection with some implementation issues of a firewall. Now we are talking about how we can implement a firewall in a practical situation. Bastion host, the name comes from the fact that it is a host which is unbreakable. Now unbreakable is a hypothetical concept. However careful you may be in designing or securing your system some hacker or intruder somewhere can always find the means to break into it. So it is only a short term solution you continuously need to keep upgrading this security features of a system to keep it protected against the attacks which are already published than which are new attacks would be coming every day. So you will have to also be alert to keep your system secure and intact.

(Refer Slide Time: 33:38)



So bastion host is essentially a separate or special system which is identified by the firewall administrator as a critical point with respect to the network security. Now here I was saying that, this is one computer in one network which is critical. Let us make it as safe and secure as we can. So security of a whole system or whole firewall will depend on the security of this particular system. So let us be very careful in why we design this system. This is what bastion host. Typically bastion host executes a secure version of operating system. Many vendors today they have a secure version of its operating system which is usually a strip down version, a smaller version. But it is quite safe and also these OSs are very expensive. This consists only of the services which the administrator feels are essential and for any kind of access some authentication mechanism is followed before users are allowed access.

(Refer Slide Time: 35:06)

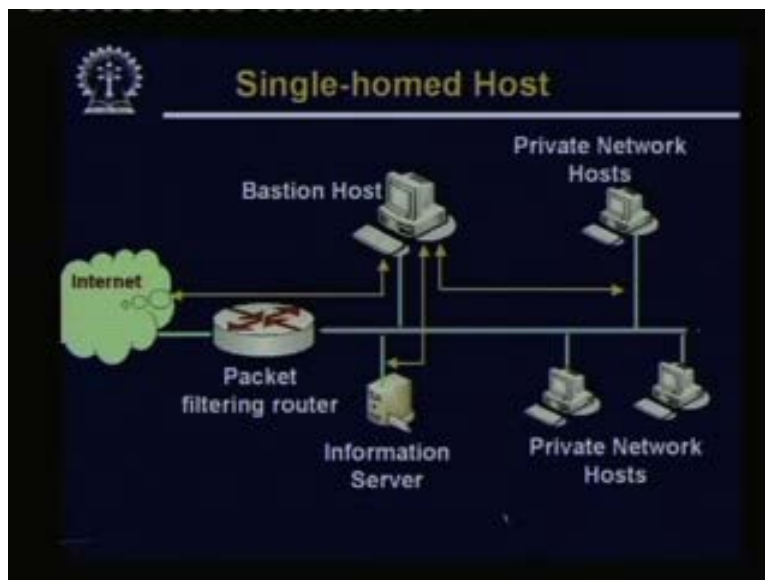


**Firewall Configurations**

- In addition to the use of simple configuration of a single system, more complex configurations are possible.
- Three common configurations are in popular use.
  - Single-homed host.
  - Dual-homed host.
  - Screened subnet.

Now shall we look at firewall configurations which uses or utilizes such bastion host in the implementation. Now there can be simple configuration of a single system. As we shall see earlier just using a single router more complex firewall configuration. They use or utilize multiple systems and we shall be seeing such complex configurations. There are three configurations which we typically find in use: single homed, dual homed and screened subnet. These are the three different alternatives for firewall implementation or configuration, whatever we call.

(Refer Slide Time: 35:57)

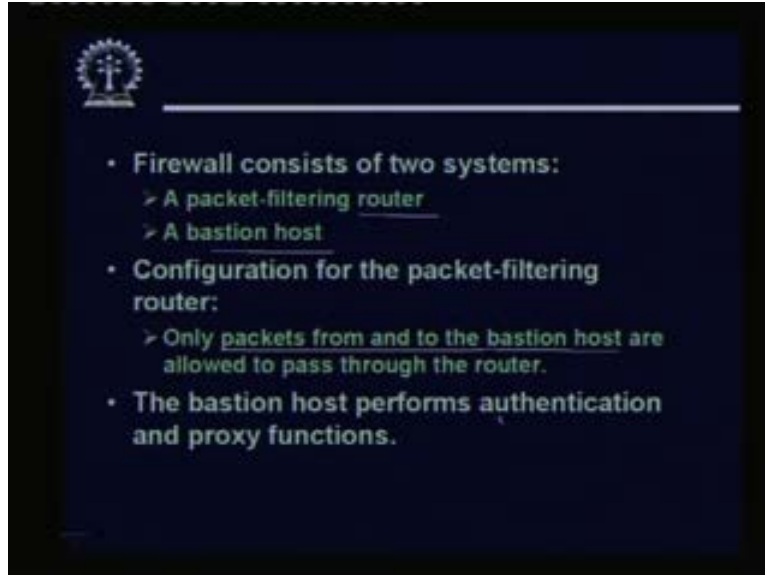


Let us start with singled homed host. This is the diagram on one side. We have the internet, this is the outside world and whatever else you are seeing, this is our internal network. Now you can see we have a router which separates the internal network from the internet. Now our internal network is represented by this bus. So this bus is our internal network. The bastion host sitting here is connected to the internal network. There are some information servers, as I said like web server or the mail server and our internal computers or private network hosts. Now you will look at this yellow arrow, the way the router and the bastion host has been configured. The router will only allow traffic to flow if it is either made destined to the bastion host or it is coming from the bastion host. Because we now bastion host is a safe and secure system. So let all communication with the outside world go through the bastion host.

The packet filtering router will block all other packets. So any packet which is directed to an internal host will be blocked. Similarly the bastion host can send and receive information from this information server. So if the outside world some node out there wants to access a white page first the request will come to the bastion host. Bastion host will forward it to the information server, then again the reverse path will follow. So similar thing will happen if an outside node wants to send some data to the internal host or vice versa. These requests have to be going through the bastion host. There is no direct path which will be allowed. Understand in order to compromise, this system you will either have to compromise or break in to the bastion host or it may be an easier proposition that you can break the router. If you can hack the router, you can easily change the packet filtering rules and once we change the packet filtering rules. So this yellow arrow that is shown they are no longer valid.

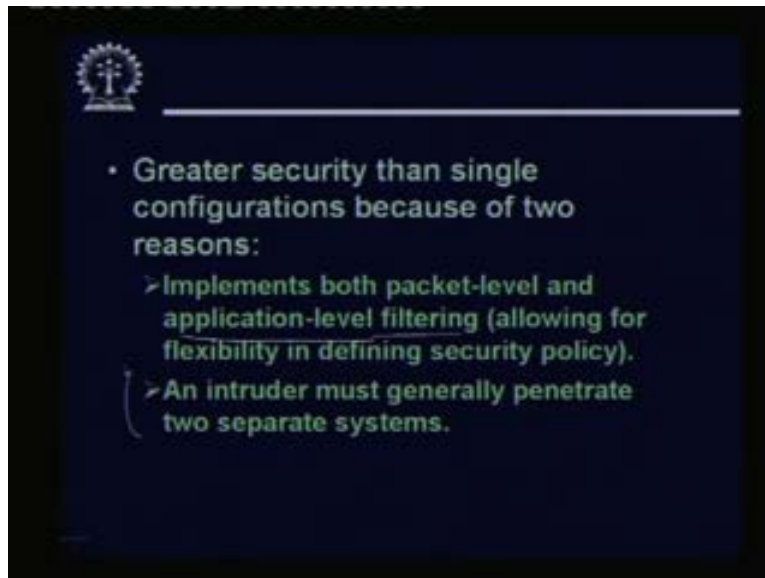
Now an outside internet host can directly start communicating with the internal network. So in the sense this configuration is not really very secure because although we have used the bastion host but the router becomes the vulnerable point in a network. Now although someone has not directly demonstrated. It is felt that the routers which are commercially available by renowned vendors like cisco. They have some deliberate vulnerable design them but still if you use them in a network, then actually you are compromising on the security of the network. So unless you have some other mechanism to safe guard the security, that means the router if it is the single point vulnerable. You can say point in the network then you are really in an uncomfortable situation. You should try to have something better than that.

(Refer Slide Time: 39:45)



So as we have seen that in this method the firewall consists of a router and a bastion host. So the router as I said it will only allow packets to and from the bastion host to flow. The bastion host can perform authentication. It can also perform the proxy functions.

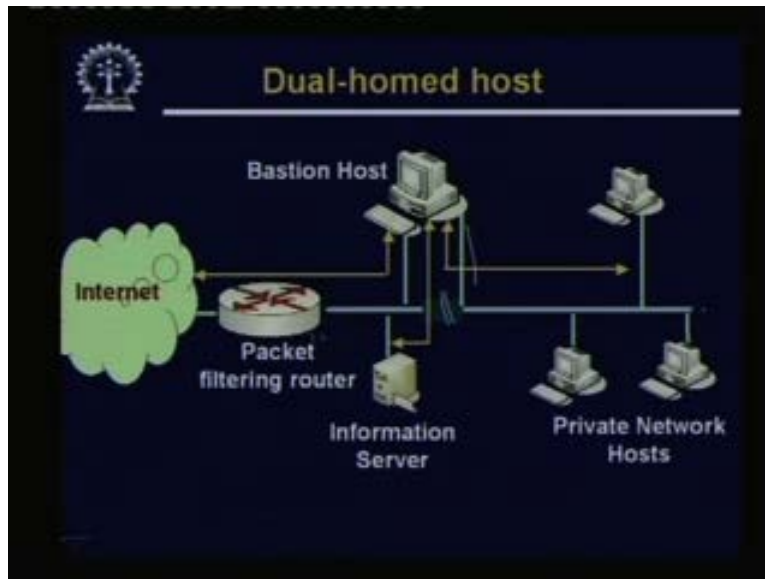
(Refer Slide Time: 40:09)



This method has greater security than single router configuration because here you can also have application level filtering or proxy filtering in the bastion host. And here although I have said that intruder can break the single system like the router. But in general you can make configuration to the other servers and systems in such a way that they will also only accept request from the bastion host. In general the intruder needs to

break the bastion host also if the internal. Administrator is very careful. So then each individual system also can be provided with some internal or personal firewall. So that only packets from the bastion host will be accepted. So that even if an intruder breaks into the firewall still that fellow will not be able to do much.

(Refer Slide Time: 41:10)



Now let us come to this second configuration. Here we are talking about a dual homed host. See dual homed host means a host or a computer with two network connections two network ports. So now we are making the bastion host as dual homed. There will be two network cards it can be connected to two different networks. So actually what we are doing here is that we are physically separating the network the two networks. Now you see the bastion host one network is connected to one to which only the information server and the router is connected and it is connected to the other where the internal private hosts are connected. So here even if the intruder breaks into the packet filter router. There is no direct path to access the internal computers.

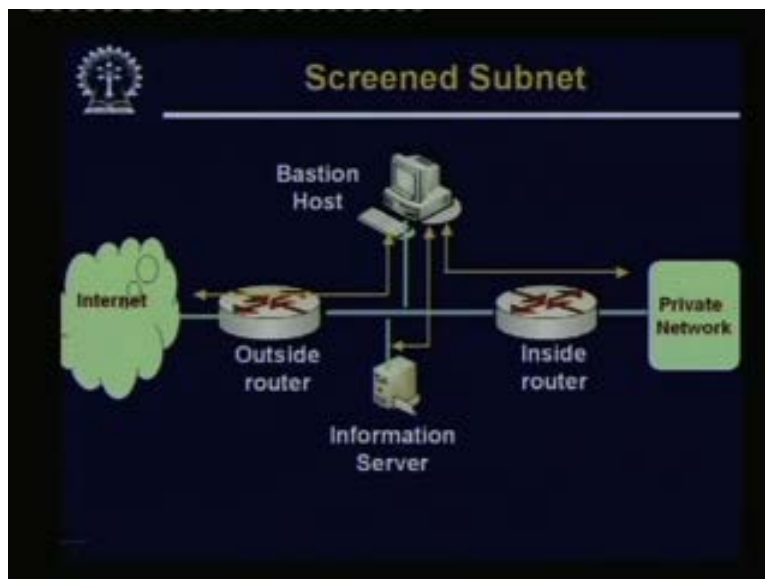
They will have to go through the bastion host. So essentially here we are forcing the intruder to also break the bastion host in order to break into our network. Just by breaking the router will not allow the person to have access to our internal hosts right. So in that sense dual homed host is an improvement of the previous approach. So here you have two separate networks with a bastion host protecting the access. Now you see here this network to which the bastion host information server and the router are connected. This is a special network . In this network some of our public servers are present like your web server mail server as I said. Now there is a special name of this part of the network. This is called a demilitarized zone or DMZ zone. So DMZ zone is also a secure zone. But it contains some information server which can be accessed from outside. So in this DMZ zone as you can see security is provided by having all accesses taking place through the bastion host.

(Refer Slide Time: 43:39)



So here the packet filtering router. You cannot completely compromise the system by compromising that. So now all traffic between internal and outside network has to flow through the bastion host. This is one very important characteristic out here. Now let us go one step further.

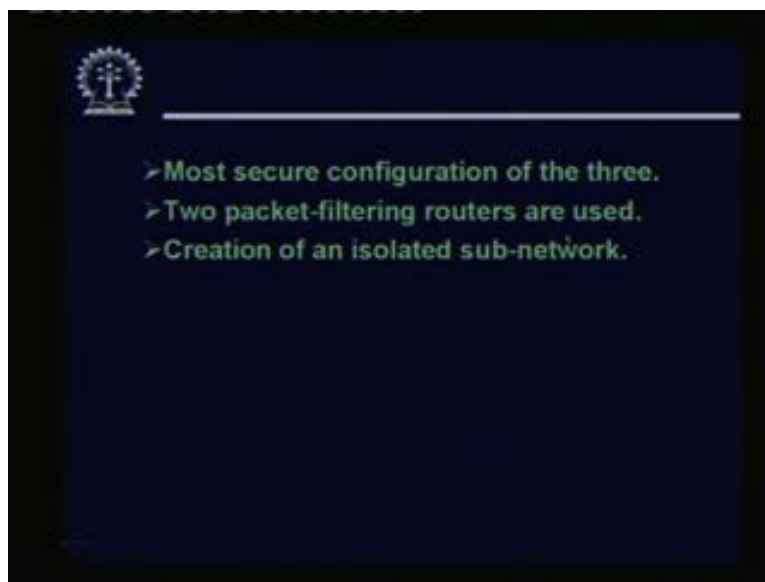
(Refer Slide Time: 44:03)



Let us have a system comprising of two separate routers because cutting network putting in two network cards. This is of course a solution. A better solution may be routers with two different kinds of policies. The internal router is protecting our private network and the external router is used as an interface to the outside world. And the bastion host and

information server are in the middle network. So as you can see the bastion host, as usual it holds the responsibility of communicating with the outside world, with the private network and with the information server and the inside router can be configured to accept packets only from the bastion host. So it is almost impossible for an external intruder to break into the internal router because the external intruder can never reach the internal router directly. So even if the external router is compromised the internal router cannot be reached because the internal router will be ignoring all packets which are coming from any other place other than the bastion host. So this is typically the most comprehensive version where this firewall system comprises of a pair of routers and a bastion host. This is called the screened subnet kind of a firewall.

(Refer Slide Time: 45:40)



Now this is the most secure configuration of the three that, two packet filtering routers which are used and it creates an isolated sub network. Now in this context let me also talk about a few things. See we have talked about a firewall that protects our network from the outside world. But as a user as a network administrator you have to look beyond this basic capability. See having a firewall in the server as part of the firewall you get a few benefits. Alright, you get a mechanism to filter some traffic you get a mechanism for the proxy function some kind of content bit based filtering you can have. You can have an online virus checking of the mails which is becoming so important nowadays. Because many of the mail attachments reach our machine with viruses. If you can check and remove those attachments automatically at the proxy server it will be very good.

So this provides some kind of a boundary protection to our network. Our network it is connected to the outside network we are putting as if a boundary wall across our network. But what if there is an intruder sitting inside what to do about it? In a big organization this is always possible and very much possible. So we are protecting we are closing all the windows and doors but you do not know whether a thief is sitting inside our organization right. So for this again there are several different technologies and



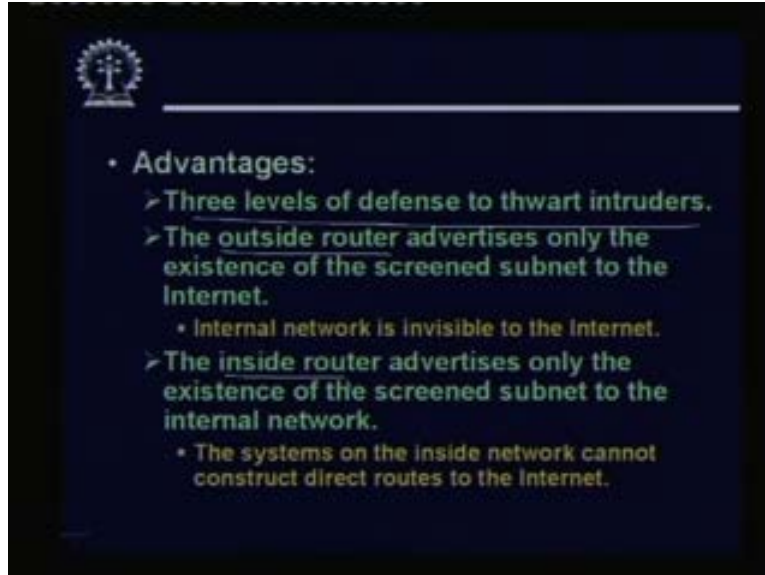
techniques which have been put to use. Now very important technique which is being used it is still a topic of research it is called an intrusion detection system. An intrusion detection system can be installed on all the main servers and some special computer systems on the network which actually continuously monitors the network traffic and primarily looks for some kind of statistical anomaly.

For example say there is a computer system which is normally expected to receive packets at a certain rate throughout the day. But suddenly someone finds that the rate of packets to that server has grown up gone up abnormally 10 times. So this is possibly an attempt to break into that server. May be some dummy packets are automatically generated by some node and has been sent to that particular server with an attempt to break into it. So this is just a simple example. There are many such attacks which are possible and each of these attacks carries some kind of a statistical signature along with them. So if you can identify the signatures and if you can basically carry out some filtering based on the signatures. So you can raise an alarm every time you feel that something wrong is probably going on.

So an ideal or an intrusion detection system tries to do exactly that. Now in addition to that you can have installed some personal firewalls on your desktops. This is also very essential in modern day computing because you need to protect intruders from breaking into your system also. Most of our personal computers and systems are insecure in the sense that it is rather easy for a well trained intruder to break into the system and gain access to very important information. So if we can have a simple desktop level firewall. It can protect us from even the internal intruders of the network. Moreover you know that there are many applications we shall be talking about this later again. There are many internet applications through which we carry out some transactions. Many of them are financial transactions.

Also they were asked to key in some confidential information like our bank account password, the account number, the credit card number and so on. There is a process called fishing which people are very worried about today where some intruders somewhere can get hold of my information without me knowing it. So this kind of things can also be stopped by a well designed personal firewall which can also include an anti-spy ware system. Spy ware is also a big problem now days. It can make our system vulnerable to external attacks.

(Refer Slide Time: 50:55)



Just continuing in this third alternative we basically have three levels of defense to thwart intruders. There are two routers; there is an outside router, there is an inside router and thirdly there is the bastion host. So the outside router makes the internal network invisible to the internet. Similarly the inside router makes the internet invisible to the inside network. So everything has to go through the bastion host.

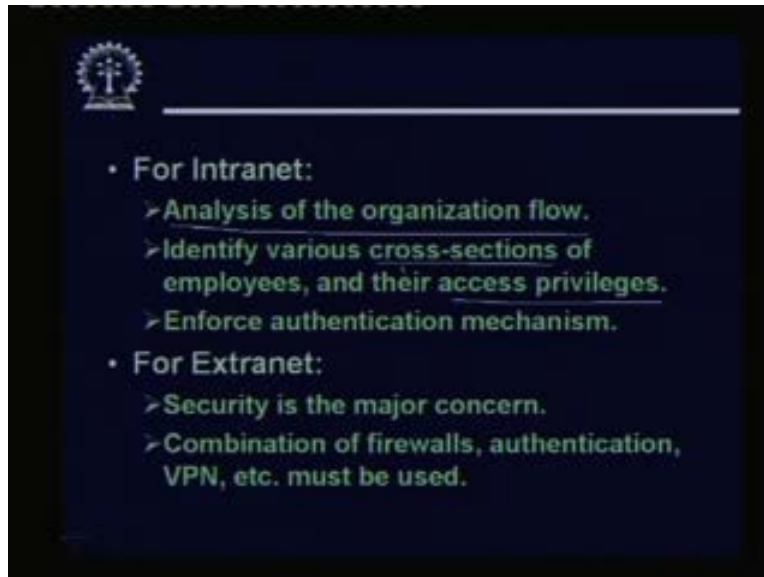
(Refer Slide Time: 51:32)



So let us again come back to the intranet and extranet problem and let us very briefly look at some of the design issues here in the intranet and extranet. Some of this we shall

be talking about some detail in our next lectures. But let us first look at some of the basic issues that you need to address when you are designing an intranet or an extranet.

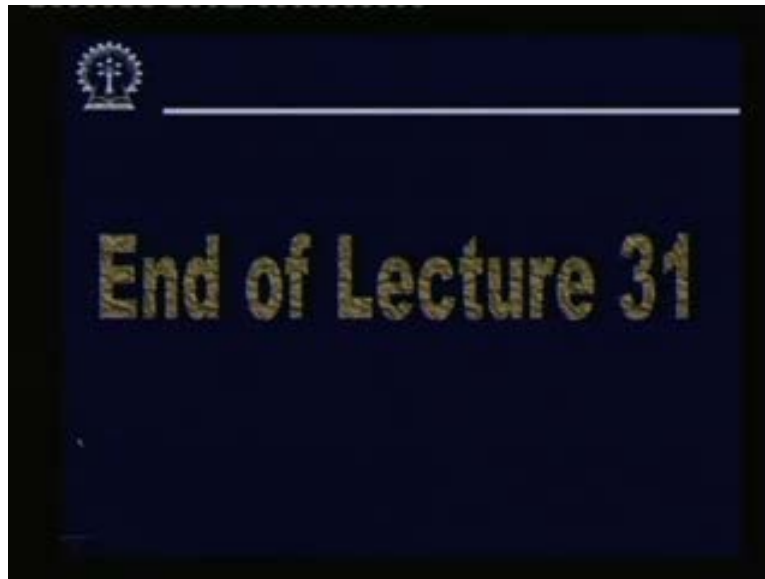
(Refer Slide Time: 52:04)



Intranet, as I said since we are trying to maintain an information system for the organization where different cross sections of the employee may have access to different cross section of the information. So some analysis of the organization flow and the different categories are cross section of the employees their access privileges should be identified. This is very important because if this process is not done, properly then some employee may be having some privileges or access to some information which they should not have. So here you should have a very flexible authentication mechanism. So after authentication the system should be able to decide that what is the kind of information this particular employee is allowed or supposed to have accessed to.

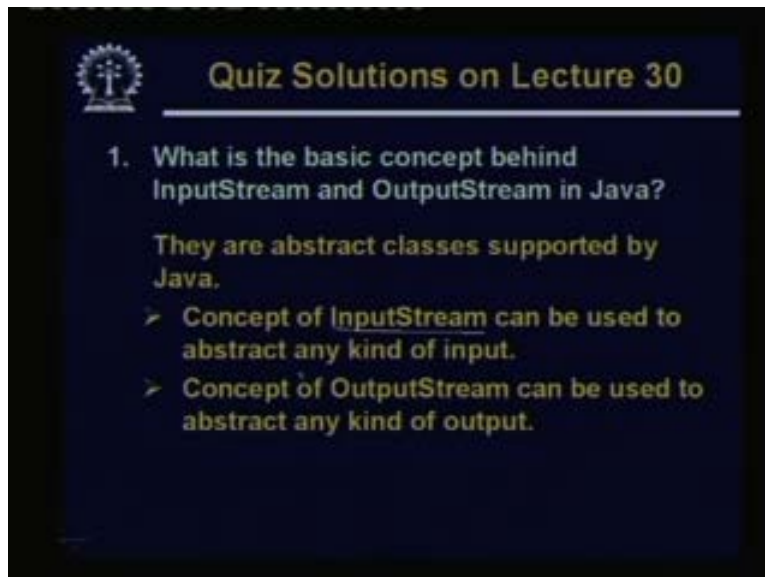
Similarly for extranet some of the issues are similar. But some of the issues are even more of concern than security. Now somebody from outside my network is trying to visit my website get some information interacts with us. And so one here some much stronger authentication mechanism should be there to validate whether that external user is an authorized user of our extranet or not. So there are many such systems in place. Unfortunately many of the systems which people use they lack the necessary security levels though they have some vulnerability. So in general we can use any combination of firewalls, some special authentication mechanisms, may be based on some kind of smart cards or some kind of biometric authentication virtual private network. So all these things combination of all these technology should be used to make extranet a safer place to carry out transaction discussion meetings and so on.

(Refer Slide Time: 54:30)



So with this we come to the end of this lecture where we have basically talked about some intranet and extranet design issues. And we have looked at the several different alternatives to firewall designs. So we shall now look at the solutions to the equations from last lecture.

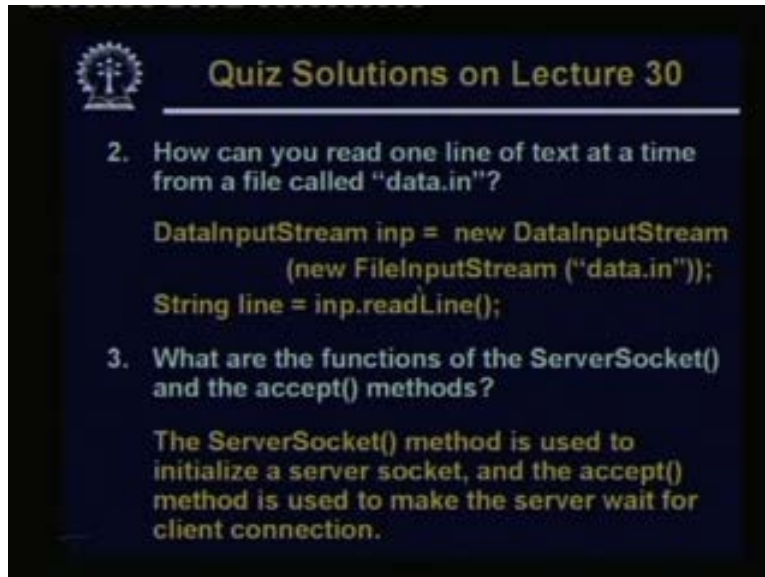
(Refer Slide Time: 54:55)



What is the basic concept behind input stream and output stream in java?

They are basically abstract classes which are present in the java supported libraries. The input stream class can be used to abstract any kind of input and outputstream for any kind of output.

(Refer Slide Time: 55:19)



The image shows a slide titled "Quiz Solutions on Lecture 30" with a logo in the top left corner. It contains two quiz questions and their solutions. Question 2 asks how to read one line of text from a file named "data.in". The solution shows Java code using DataInputStream and FileInputStream. Question 3 asks about the functions of ServerSocket() and accept(). The solution explains that ServerSocket() initializes the server socket and accept() makes the server wait for a client connection.

**Quiz Solutions on Lecture 30**

2. How can you read one line of text at a time from a file called "data.in"?

```
DataInputStream inp = new DataInputStream  
    (new FileInputStream ("data.in"));  
String line = inp.readLine();
```

3. What are the functions of the ServerSocket() and the accept() methods?

The ServerSocket() method is used to initialize a server socket, and the accept() method is used to make the server wait for client connection.

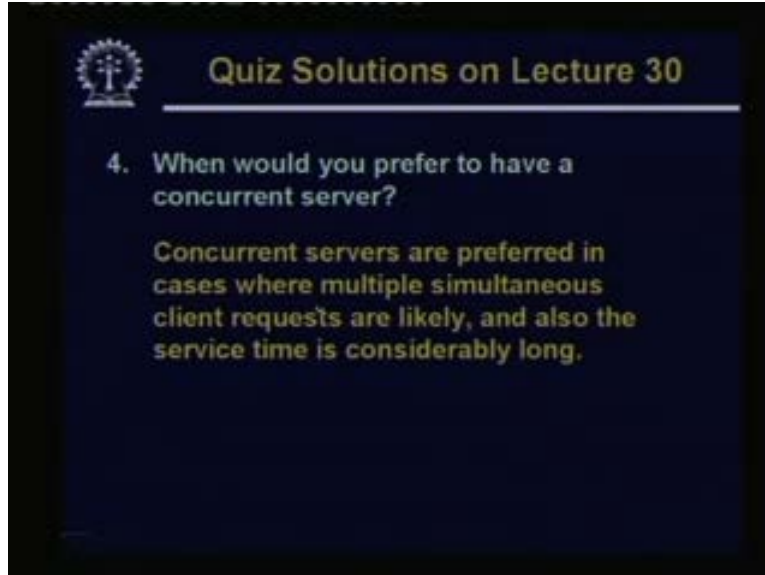
How can you read one line of text at a time from a file called data dot in?

Well first you can use the file inputstream to create new instance of an object. Then you can call data input stream to create an object inp using which you can call the readLine method. This is how we use.

What are the functions of the serversocket and the accept method?

The serversocket method is used to initialize a server socket while the accept method is used to make the server wait for the client connection. So the server will be blocking itself and executing accept and will be waking up as soon as the client connection request comes.

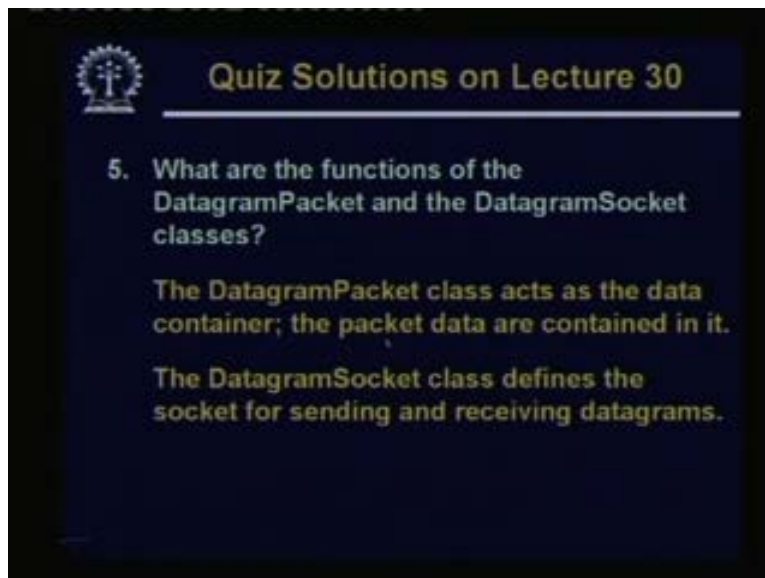
(Refer Slide Time: 56:04)



When would you prefer to have a concurrent server?

Concurrent servers are preferred in cases where multiple simultaneous client requests and also the service time is long.

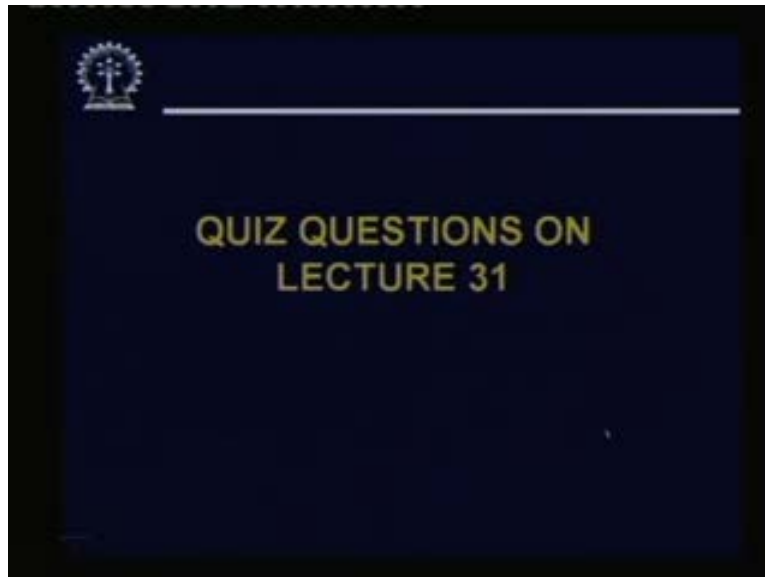
(Refer Slide Time: 56:21)



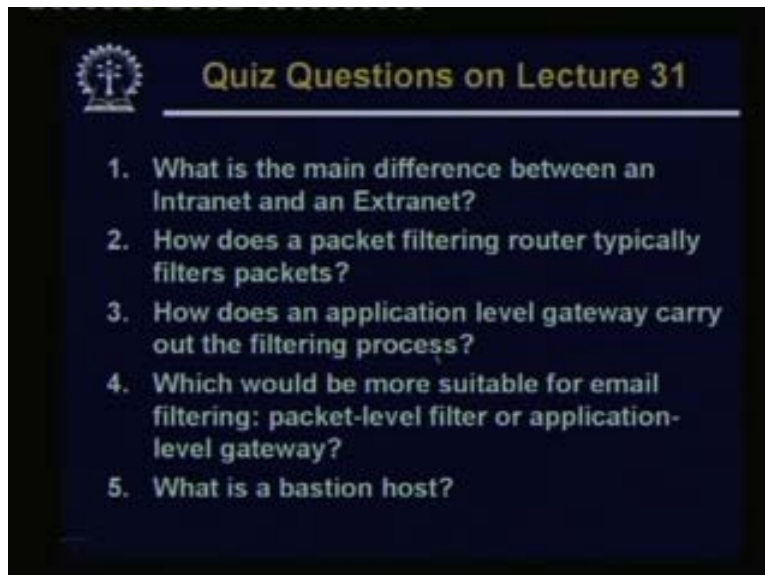
What are the functions of the datagrampacket and the datagramsocket classes?

These as I said the datagrampacket class access the data container the packet data contained it represents the packet. Whereas the datagram socket class defines the socket for sending and receiving datagrams. This is the difference. So now some questions from today's lecture.

(Refer Slide Time: 56:45)



(Refer Slide Time: 56:46)



What is the main difference between an intranet and an extranet?

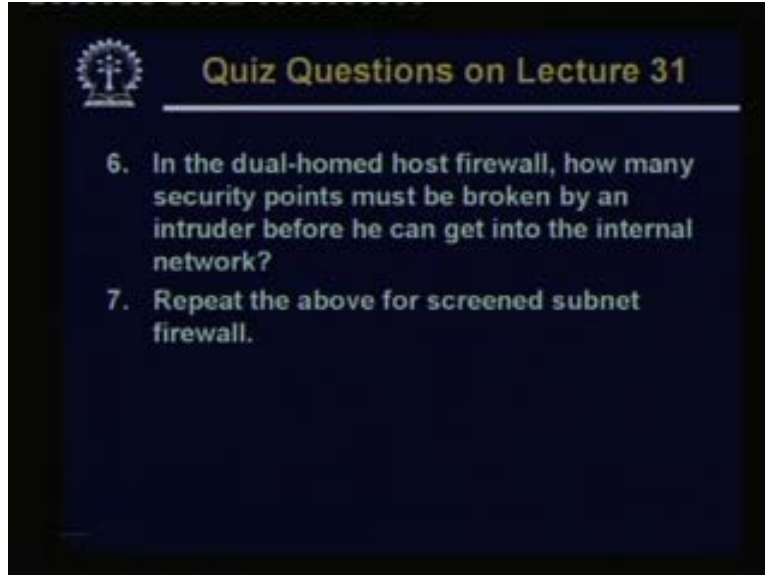
How does a packet filtering router typically filters packets?

How does an application level gateway typically carry out the filtering process?

Which would be more suitable for email filtering packet level filter or application level gateway?

What is a bastion host?

(Refer Slide Time: 57:13)



In the dual homed host firewall how many security points must be broken or bragged by an intruder before he can get into the internal network?

Seventh one is the same problem but for the screened subnet firewall.

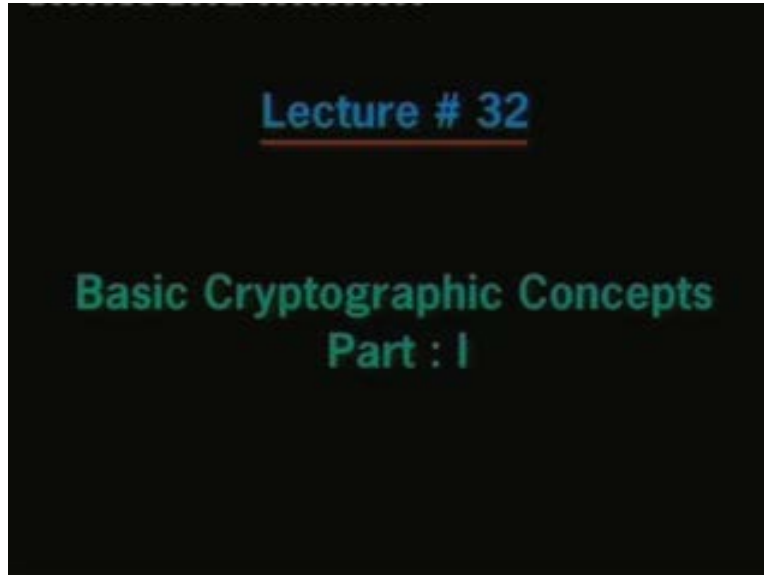
So in the next lecture we shall be starting our discussion on some basic cryptographic techniques which can be used for network security. Till then good bye.

(Refer Slide Time: 57:48)





(Refer Slide Time: 57:52)



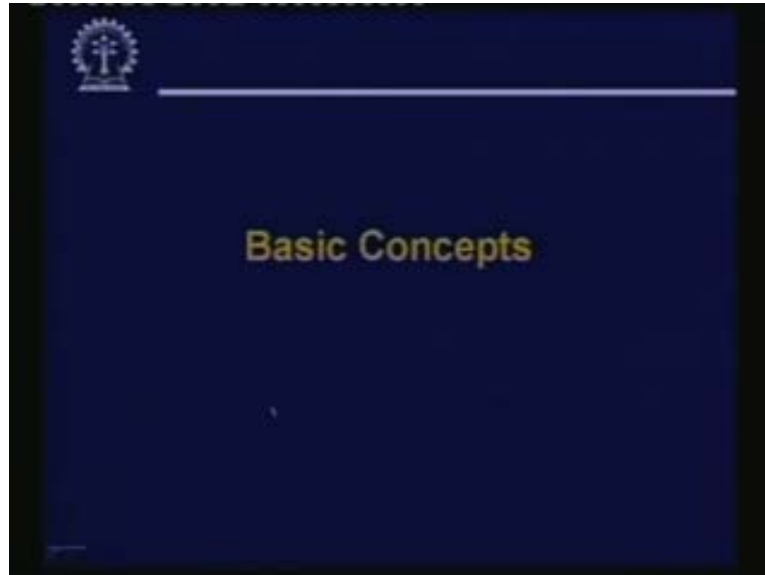
In this lecture we shall be continuing with our discussion on network security. If you recall in our earlier lecture we had talked about intranets extranets and firewalls. Now today in the lecture first we shall talk about some of the general network security threats that we typically encounter followed by some discussion on some basic cryptographic techniques.

(Refer Slide Time: 58:29)



So let us start by some of the basic concepts in network security.

(Refer Slide Time: 58:32)



(Refer Slide Time: 58:38)

A slide with a dark blue background. In the top left corner, there is a white logo of a tree inside a circle. The title "Security Attacks" is written in a yellow, sans-serif font in the center of the slide. Below the title, there is a list of bullet points in white text:

- Any action that compromises the security of information.
- Four types of attack:
  - Interruption
  - Interception
  - Modification
  - Fabrication
- Basic model:

Below the text, there is a diagram showing a horizontal line with a circle containing the letter 'S' at the left end and a circle containing the letter 'D' at the right end. Below the 'S' circle is the word "Source" and below the 'D' circle is the word "Destination".

We start with the different kind of generic security attacks that we typically encounter in a network or in a computer system.