

**Computer Networks and Internet Protocol**  
**Prof. Soumya Kanti Ghosh**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Lecture - 60**  
**Network Security – III [TCP/IP Security]**

Hello. So, we will be discussing on Network Security or rather we will be continuing our discussion on network security; for last couple of lectures we are discussing about network security what are the different aspects of the security. So, today we will see some of the things which are more related to TCP IP layer alright. So, as we mentioned that security per say is a phenomena which need to be ensured across the layer right like it; like they are stacked in at different levels like starting from top from application layer to the physical layer.

However, security comes as a vertical type of things right it is some sort of a end to end phenomena should be there otherwise it is; making it fully effective will be very difficult right. So, and as also we understand that when we the TCP IP or OSI model came up and when or the devices or which are communicating based on these protocols which are defined for different layers, they are not initially made for security purpose right; they are made to communicate um.

And whenever we put any security aspects, that becomes more as a hindrance to that things right. Once you any say for physical security also if you go on checking, the traffic flow decreases, the number of processes increases and type of things. So, that is need of more computational power, need to handle this congestion and type of things will come into play right.

So, so there may be some devices which are security enabled; that means, they understand that what is a security, some devices which are still not security enabled right. So; that means, if you if you if we change the basic protocol stack or the format; then some of the intermediate devices may fail to understand that what is what is their interventions; in others sense it may drop the packet like say IP packet. IP packet has a specific format or specification based on the guideline or the protocol standardized standard protocol. Now for the security purpose embedding the security if I change this

IP packet; some of the routers may not be able to understand that what is there in the IP packet.

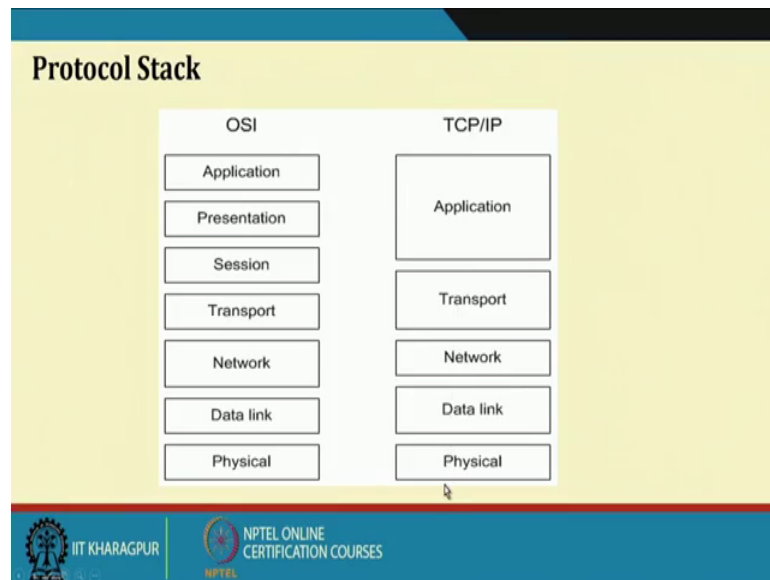
In other sense it may drop; it will drop the packet it will not recognise the IP packet. So, whatever we do with this stack protocol stack whether OSI or TCP IP; we need to keep in mind that a device which is not able to decipher these security information should be able to forward this packet right; as it was doing earlier right. So, the whole process came up like that.

Another thing we will see slowly another thing is important see; if we look at the whole protocol stack; so, there are different layers right known application layer if I look at the TCP IP protocol stack what say, so there is a application layer, then transport, then IP, then data link and physical layer right. So, these are have a peer to peer connectivity right transport layer of system 1 when we are communicating to a system 6 in something that is a peer to peer connectivity.

So, the security at that level should have a also a peer to peer way of handling that or connectivity or handling those security things that has to be there right. So, with this notion let us look at that what are the different aspects of security of means today's networking and the need of security need not to be explained again. And we do understand means from a personal day to day experiences or working experiences in office and other e platforms we understand there is a security is a must phenomena which need to be there.

So, today mostly we will be concentrating on TCP IP security has to have it has a back to back things for the OSI. So, if we look at our common OSI TCP IP protocol stack; so there are here 7 layers or here 5 layers know.

(Refer Slide Time: 05:03)

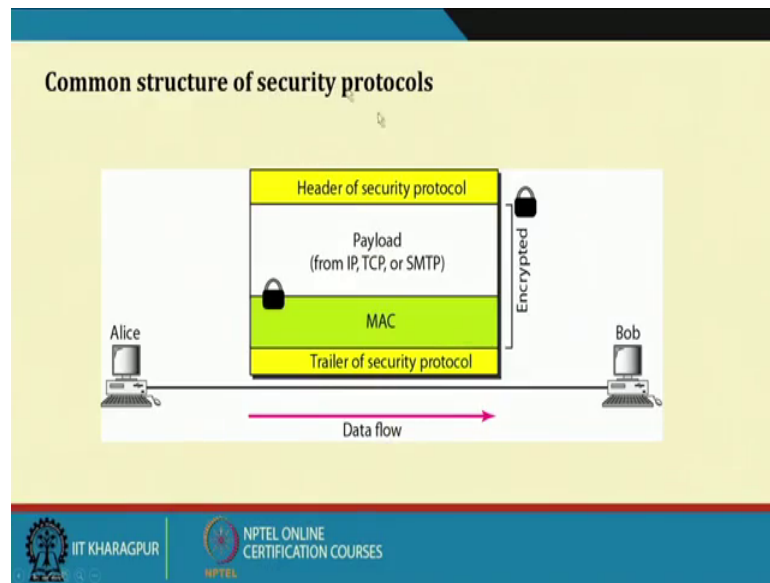


Now see what we try to say that one is that there should be an end-to-end phenomena if you want to put security in the things. Another thing you see physical layer is basically a connectivity right; in some of the cases physical layer is not in some (Refer Time: 05:23) is not considering the protocol stack; it is more of a communication phenomena right.

So, any way that it is a point-to-point means hop-to-hop connectivity here also data link layer hop-to-hop connectivity. So, per say the security of this traffic is something under the jurisdiction of some authority right like if the; if the physical layer layout in the IIT, Kharagpur; so, that is within the administrative control of the IIT, Kharagpur authority and there is a more physical security is most required that it is not tempered and type of thing. Similarly data link layer is also hop-to-hop connectivity; so, as such the security of these is also not what we say a wide concern as such because it is a only hop-to-hop things type of things it can be ensured by the 2 communicating party right.

The challenge has come from the network here right because you have a path which is not exactly in your control; it is outside your network and it you do not know that the path which are the routers and other devices intermediate devices it is following. So, from that context what we see that from network layer transport layer application layer; here the security phenomena are more predominant. So, our discussion will be more concentrating on this that what are the different phenomena or what are the things we put it in different literature and so and so forth right.

(Refer Slide Time: 06:51)

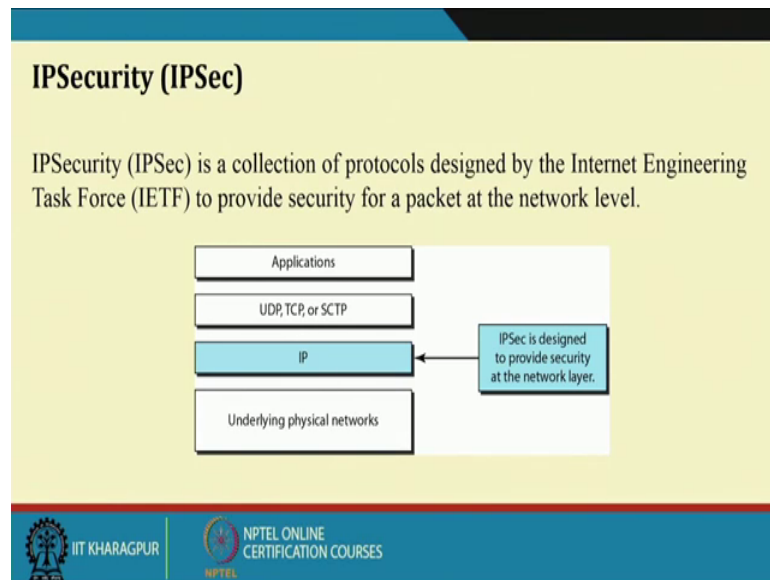


So, if you look at the generic protocol stack. So, there should be these are the different standard layer that IP, TCP, SMTP is the application layer and type of things and below that there is a MAC is there and the trailer security protocol and things. So, this is this MAC is not your; this MAC is not basically the MAC what we have seen in the layer 2. So, this is more message authentication code or the code which is required to authenticate this message and type of thing right.

So, in other sense what we say this becomes encapsulated in a bigger packet; which has a header for the security protocol trailer for the security protocol, but the overall packet when moves along a layer it should be able to decipher by a router or a device which is not security enabled right; which is not able to understand this what is this high header security protocol or trailer security protocol, but still it is able to able to forward this packet otherwise it will drop the packet right.

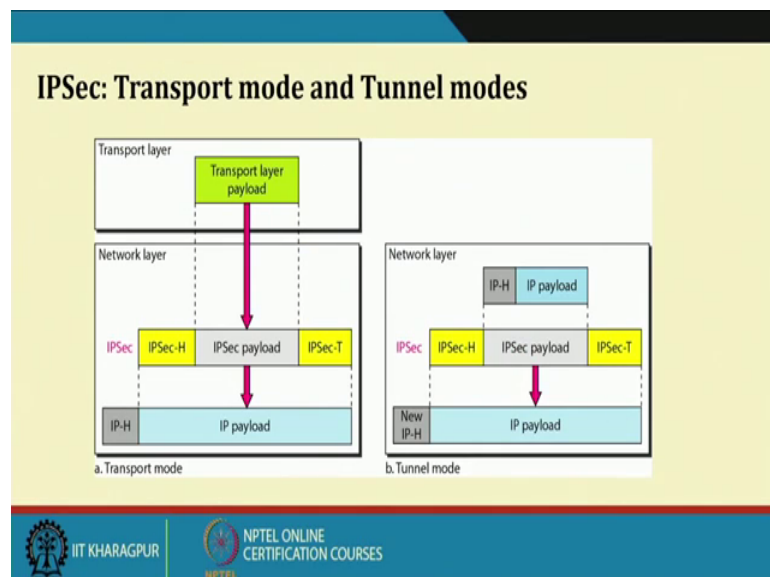
So, any layer any layer say it whether it is IP or transport or application has to follow this philosophy. So; that means, the actual packet is somewhere encapsulated along with the wrapped along the security things.

(Refer Slide Time: 08:25)



So, IP level the IP security or IPSec is the predominant protocol is a collection of protocol designed by the IETF to provide security packets to the network level; so, this is IPSec designed to provide security level. In other sense it is instead of IP it is IPSec and the other layers basically able to intercept interpret that things in the similar fashion.

(Refer Slide Time: 08:53)



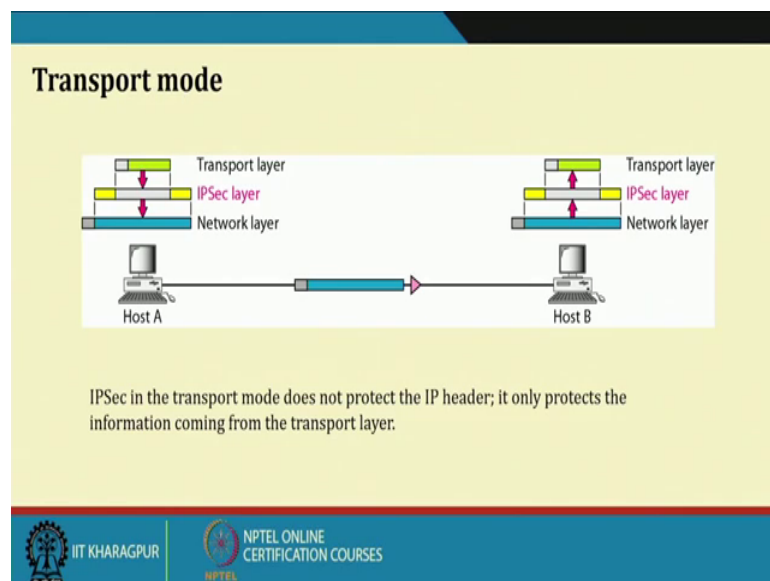
So, there are 2 mode of 2 modes for IPSec one what is called transport mode, another is the tunnel mode; so, these 2 mode of communication. So, in case of transport mode the transport this is this transport mode is related to the IP layer not the transport layer per

say. So, these becomes a payload to the thing right and it is if the actual IP header comes in the form (Refer Time: 09:22) and the IPSec header and trailer are added.

So, primarily it protects the payload or in the transport layer payload of the things right. So, it is transported across the network so, but the IP header is not protected; in a in case of a IPSec tunnel mode here the IPSec header IP header is updated to a new IP header; so, that is also protected. So, it is sort of a virtual tunnel is made between these 2 parties and the things goes to the things right.

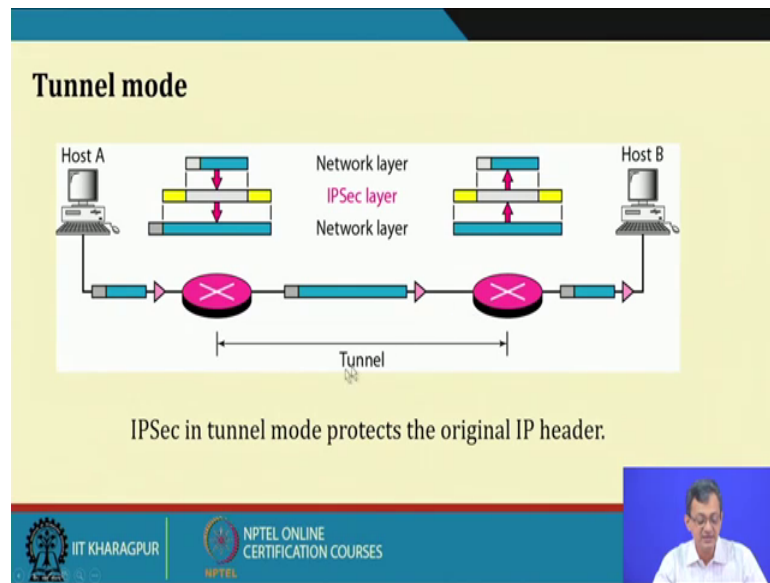
So, only thing we need to take care there are some of the fields which are mutable or some of the fields that is source destination etcetera has to be taken care at the new IP header. We are not going to the details of the protocol it is left to you to those who are interested can look into the things, but we this is the basic philosophy.

(Refer Slide Time: 10:15)



So, in transport mode IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer or the payload which is getting from the things right here the it is structure is like this; so, it is there at the host B it is deciphered or extracted in this per say.

(Refer Slide Time: 10:35)



Whereas, in case of tunnel mode protects the original IP header because it comes with a new IP header and moves like that; so, it is a form a tunnel thing between the 2 devices or 2 parties.

(Refer Slide Time: 10:49)

### IPsec services

Services	AH	ESP
Access control	Yes	Yes
Message authentication (message integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

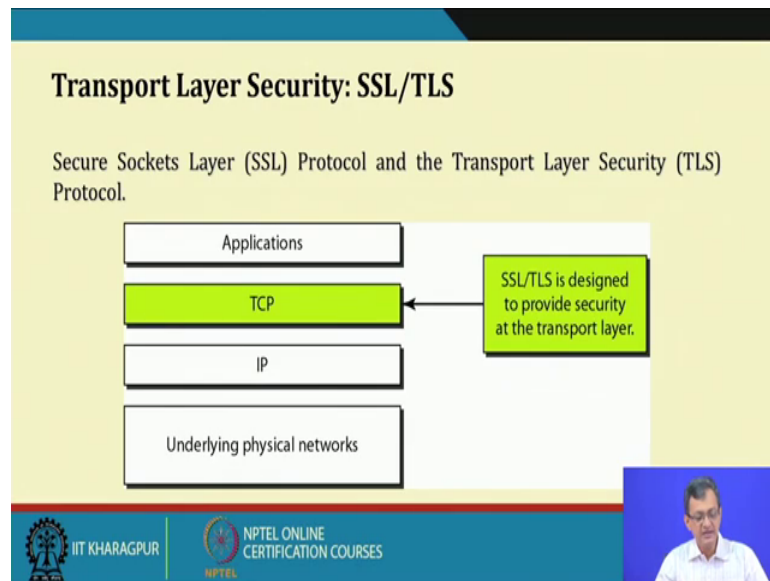
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, there are different services access control, message authentication or message integrity, entity authenticity confidentiality, replay attack protection these are supported by this. So, this AH and ESP we are not going into details; so, the things that those are

some of the things like authenticated; authentication header and encapsulated security protocol header ESP header.

So, these are the things to type of headers what the IPsec will have; we are not going into those formatting, but there are different services which can provide and ESP can provide. But if we even keep this part allow; so we can see these are the IPsec related services which are provided by the IPsec right.

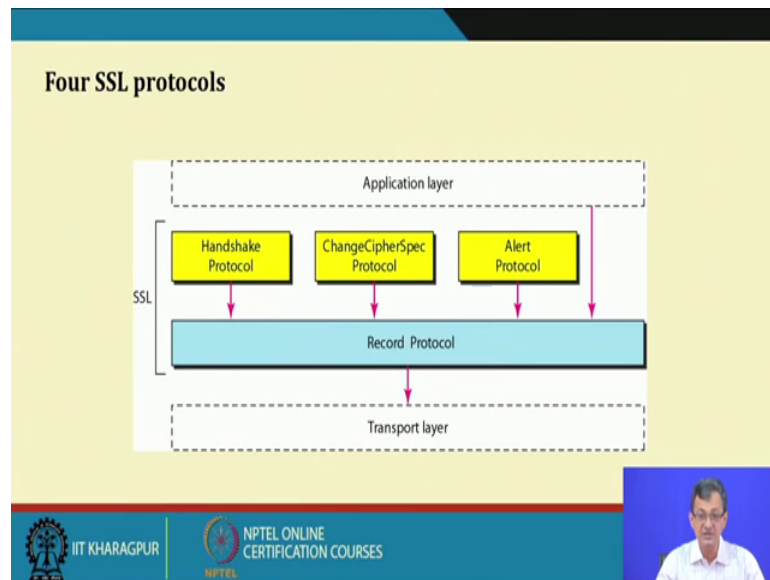
(Refer Slide Time: 11:35)



Next come transport layer security or SSL or TLS. So, we are used to the SL SSL; so this was the generic version or the IETF supported version or standardized version is the TLS its of the of the SSL basic protocol. So, it acts on the TCP; so, it basically provides security at the TCP level. So, it is designed to provide security at the transport layer. So, it goes on and at the peer transport layer should understand that how to extract the secured information; so, this is the SSL or TLS type of traffic security.



(Refer Slide Time: 12:19)



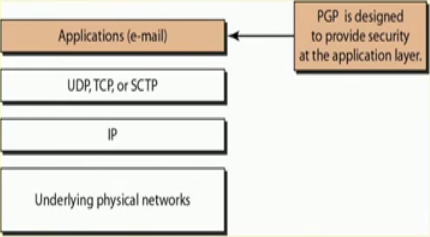
So, there also 4 protocols or sub protocols are there handshaking protocol. So, have some negotiation between the parties there is a change cipherspec protocol for finding out that which is the what sort of cipher parameters or the things will be there. There is alert protocol for any type of alert generation things and finally, the record protocol which basically handles the thing and talk with the what we say integrate with the basic transport layer.

So, again we are not going details into those things. So, these are the different type of 4 protocols; 4 sub protocols as you say that the at the SSL or TSL level which allows it to handle the scenario right; so, 4 SSL protocols.

(Refer Slide Time: 13:11)

### Application Layer Security: PGP

One of the protocols to provide security at the application layer is Pretty Good Privacy (PGP). PGP is designed to create authenticated and confidential e-mails.



The diagram illustrates the TCP/IP stack with four layers. From top to bottom: Applications (e-mail), UDP, TCP, or SCTP, IP, and Underlying physical networks. A callout box on the right points to the top layer, stating "PGP is designed to provide security at the application layer."

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

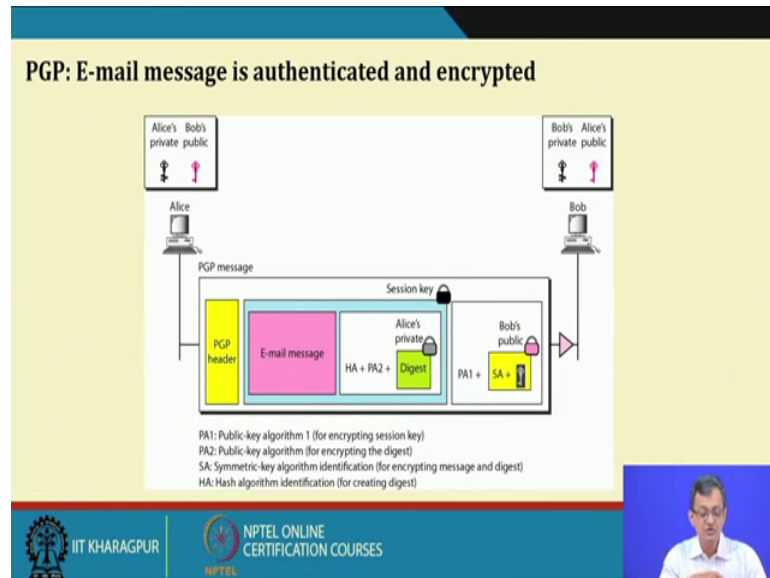
So, this provides a security at the transport layer the other thing is the application layer or PGP protocol. Like PGP is a example scenario that is say in application layer; these are the applications which are talking to each other right. So, there is a server application, there is a client application which talks to each other this can be mail application this can be something say FTP type of file transfer application, this can be something which is DECP or type of DNS type of application; so, there can be different sort of applications which can be there. Now, this the application is there has the different type of requirement at there in. Now in order to handle those requirements; so, there are way it handles the security aspects may differ from one to another right.

And the other the major one of the I should not say means I should; I it maybe advantages or convenience for the application layer is the application layer talks to the application layer it has a more resourceful layer where you can do security decipher at the other end type of things right. So, at the; at the top it is a layer 7 or layer 5 in the TCP IP protocol OSI or TCP IP protocol.

So, that way application layer may be more resourceful thing. So, in these case it is a reference is from the pretty good privacy that is a PGP protocol for mail transfer. So, PGP designed to create authenticate and confidential emails right; so, pretty good privacy email transfer the PGP protocol is there. So, this is a example scenario or typical

scenario where these security can be and the security of the of the application layer can be demonstrated.

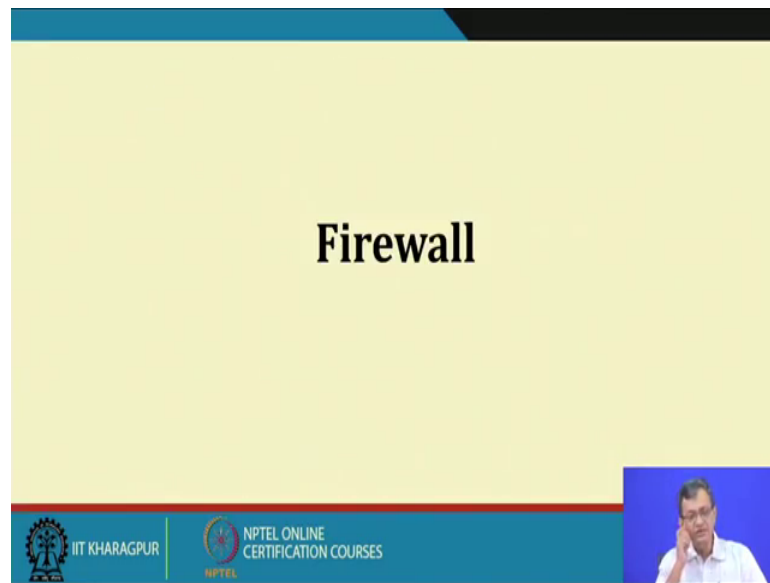
(Refer Slide Time: 15:21)



So, if you if you look at that PGP protocol per say; so, there are email message is authenticated and encrypted. So, it is a something at the at the email message it is hashed and a digest is created over that the encryption thing is there; that there is a session key which is passed to the which is generated. So, it is Alice and Bob are communicated; so, to communicating. So, Alice private key is embedded or encrypted with a onetime session key and pass to the other end and the on the other end Bob decrypt it and work with that protocol with the key.

So, what we see here that I can basically create a message and encrypt it or encapsulate it with appropriate crypto phenomena and then communicate to the other end to decrypt it the thing. Now this is possible at the application layer because the application layer has lot of resource and the things and it can be guaranteed, it can be shown that these 2 what level of security it provides that the message cannot be deciphered right. So, this is at the application layer and if there are different other type of application layer protocols; they may have some variant of the thing, but the basic philosophy remains the same.

(Refer Slide Time: 17:03)



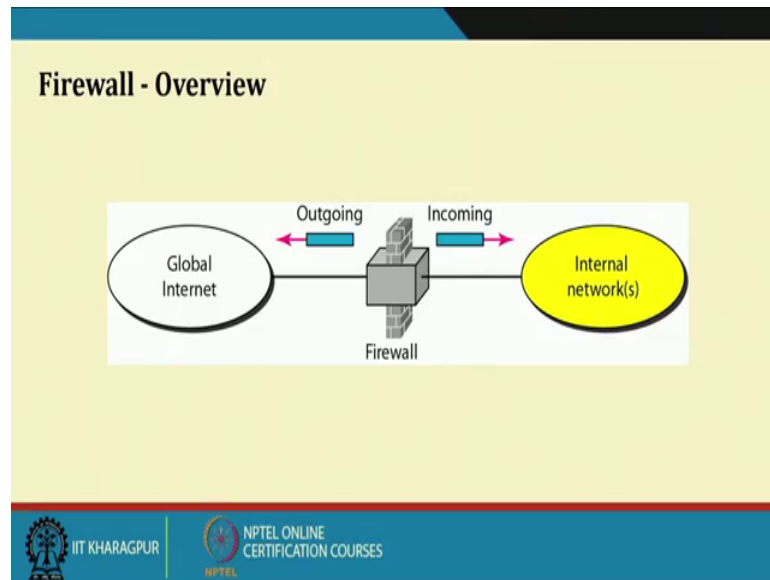
Now, with this thing we come to a phenomena like. So, we have the standard layers from one end the standard layers at the intermediate sources. So, I I need to put the security at the layer wise because the whole protocol understand where as the peer to peer connectivity.

Now the intermediate devices say I have a router which is not IPSec enabled right; so, either it has to drop the packet if it does not understand what is the header or it need to handle the packet as the as it is going through the things. Now, the if the router it may understand this is the packet, but it may not be able to decipher what is inside because that is the payload it may be encapsulated. But if the header is tampered or header is changed in such a way that the intermediate router does not understand; if it is not IPSec enabled then it will drop the packet. So, those are things need to be taken care at every layer that what it is done.

So, another thing what we have seen that on the network layer onwards the things are more externally or what we say in a more in a distributed fashion or distributed control things are there right. So, there is more security is more important whereas, in the data link layer or the physical layer that is more internal controls are there right. So, these are the 2 things with this we come to another phenomena called firewall which are we are accustomed with we here at the layout say a network or a organisation network should have firewalls.

So, firewall as the name suggest it protects the internal network from the external attack right; it can be both way also some of the things going out of this firewall also can be handled. So, it is a something a logical wall between the 2 networks right.

(Refer Slide Time: 19:13)



So, if we look at in a broad sense; so there are outgoing (Refer Time: 19:17) to the global internet and this is my internal network and there is a traffic which is coming to the internal network. So, these are the 2 broader way of looking at it.

(Refer Slide Time: 19:29)

- ### Firewall
- Firewalls are effective to
    - protect local systems;
    - protect network-based security threats;
    - provide secured and controlled access to Internet;
    - provide restricted and controlled access from the Internet to local servers.
- IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now, firewalls are effective to protect local systems or meant to protect local systems, protect network based security threats, provide secured and controlled access to internet provide restricted and controlled access to the internet to the local thing right. So, all all type of things; try to protect the local system, protect network based security threats which are network enabled security threats provide security and controlled access to the internet right.

So, that is for outgoing traffic for incoming traffic provide restricted and controlled access from the internet to the local servers or systems right. So, this is the overall the how the firewall as supposed to do right. Now, obvious question may come that which layer the firewall works right; whether it is works in the IP layer, transport layer or some other layers etcetera.

(Refer Slide Time: 20:29)

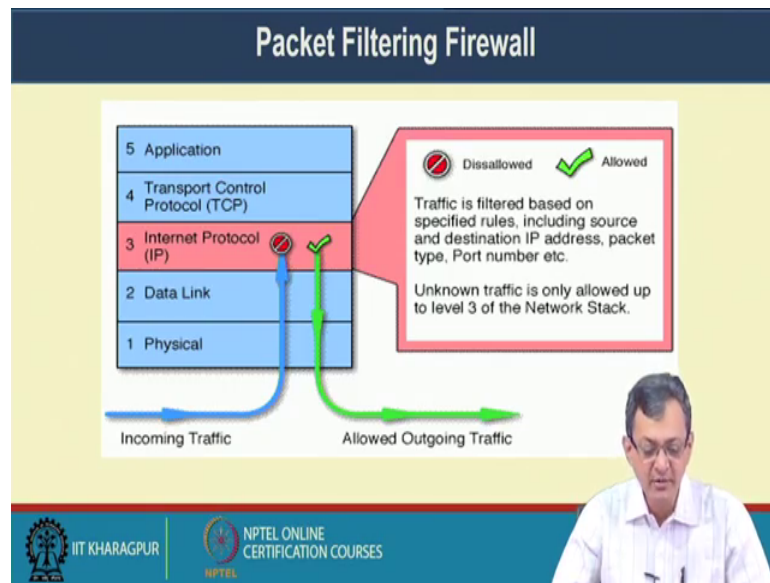
The slide is titled "Types of Firewalls" and lists three types of firewalls:

1. Packet filters
2. Application-level gateways/ Proxy Firewall
3. Circuit-level gateways

The slide also features the IIT KHARAGPUR logo on the left and the NPTEL ONLINE CERTIFICATION COURSES logo on the right. A small video inset in the bottom right corner shows a man speaking.

So, accordingly if we look at that there can be different variety or flavours of firewall. One is packet filter one is application level gateway or sometimes also a proxy firewall, another is circuit level gateways or circuit level firewalls here we will see one by one.

(Refer Slide Time: 20:49)



So, if in case of a packet filter we want what we want to do? We want to filter the IP packet based on my policies. So, firewall say if we if I say that it filters traffic between this outgoing an internet on what basis? So, there should be some policy. So, there should be some policy some implementation of that policies in this firewall by based on which it filters the traffic right; so, that that is the thing we need to have.

So, in case of a packet filter firewall; so, traffic is filtered based on the specific rules right including source and destination IP address, packet type, port type etcetera. So, these are things which are filtered based on the this rule. Now if we if you see it is not only IP layer, it also have some thing do with the transport layer. So, never the less, but it does not look at the application type of things; so, IP plus transport gives me the things. So, unknown traffic is only allowed to a level particular level in the network stack etcetera. So, it is allowed up to this and it is checked either it is blocked or passed to the outgoing traffic.

(Refer Slide Time: 21:59)

### Packet-filter firewall

Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

A packet-filter firewall filters at the network or transport layer

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, if you if we see that there are 2 interfaces of a particular packet filter firewall and this is the maybe the rule. So, any source IP this one anything is allowed or this anything coming from these are allowed or say blocked; so, which way the things are there it is allow or block or anything coming for destination port 23 are blocked anything coming for source port, so, let us see that this is the allow list.

So, anything coming from IP address source it is allowed, anything coming from the for destination 23 is allowed anything any; request coming from this destination is allowed or IP port any source IPs port 80 is allowed; that means, if it is allowed that the HTTP traffic.

So, it allows the HTTP traffic to go out nothing else; it allows any type of traffic to goes in and type of things. So, that the thing is that is the this is the allow metric though it allow the things. The other way in this form I can basically restrict the how things are going. So, it is something which is called which is also synonymous to this access control lists like so, how this access to this internal systems will be done this access control list.



(Refer Slide Time: 23:25)

**Packet Filtering Router (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).

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now, packet filter router packet filter router or packer filter firewall a applies set of rules for incoming IP traffic and then forward the and discard traffics filter traffics on both direction. The packet filter typically setup for a list of list of rules based on the matches with the IP or the TCP header; that means, IP address port number etcetera; so, it can discard or allow or forward.

(Refer Slide Time: 23:53)

**Packet Filtering Router (contd.)**

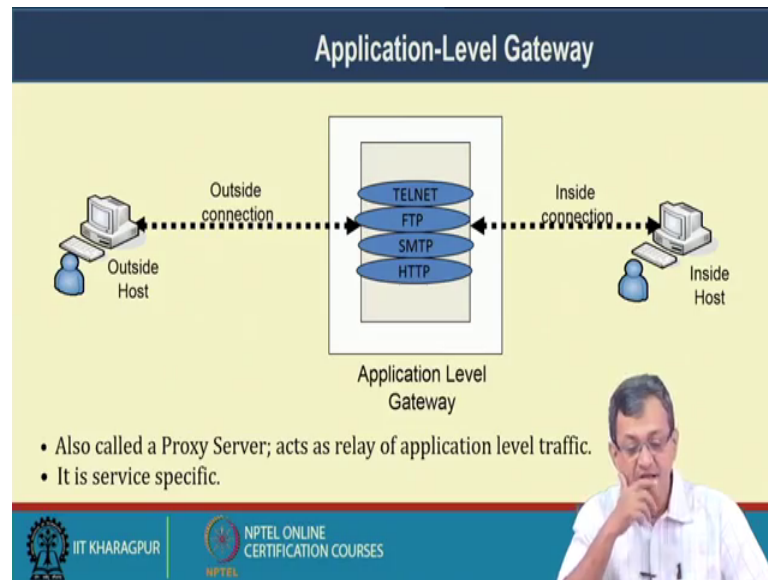
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of authentication

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, advantages simplicity transparency to user, higher transparent to user, higher speed disadvantage difficult for setting up packet filter rules right; so, what should be the

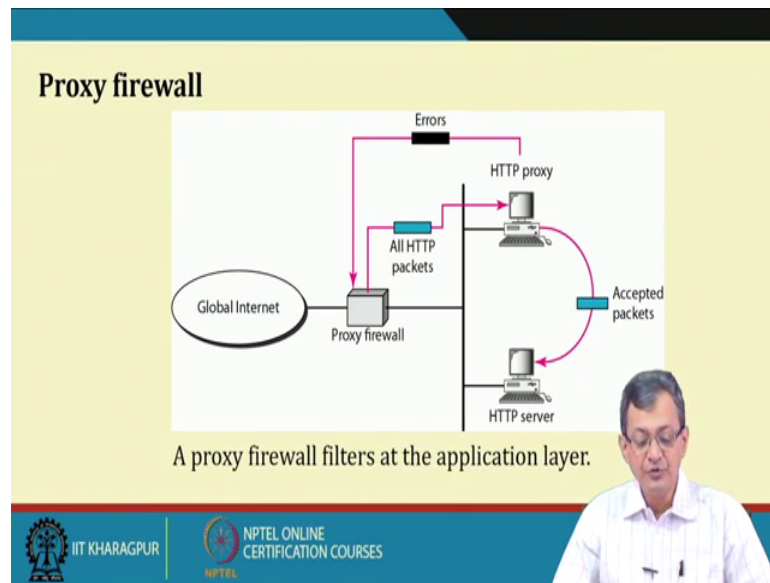
packet filters rules a large organisation may have, huge amount of IP or subnet blocks and then setting these rules are combustion and lack of authentication whether the source is authenticated source authenticated etcetera are not there.

(Refer Slide Time: 24:19)



The next come the application level gateway or at the higher level. So, it is also something proxying or the proxy firewall as relay of application level traffic right. It is service specific like telnet ftp SMTP HTTP has different type of requirement and things so that so it is service specific. So, similarly traffic is filtered based on specified application rules such as specified applications; such as a browser or a protocol FTP and combination of those things and type of things; so, that is at the higher level.

(Refer Slide Time: 25:03)



So, if we see that a typical HTTP firewall; so, if it request comes it goes to that all HTTP packets to this thing; if there is a error it goes to the return back to the firewall or it is not allowed otherwise it is accepted packet to the HTTP server to serve the things. So, that is every traffic coming for this HTTP is pushed into the HTTP firewall right; like we look at the mail security every traffic come to that that mail security firewall which takes a call that whether it is a correct traffic or not right; so, that is the way it works.

(Refer Slide Time: 25:41)

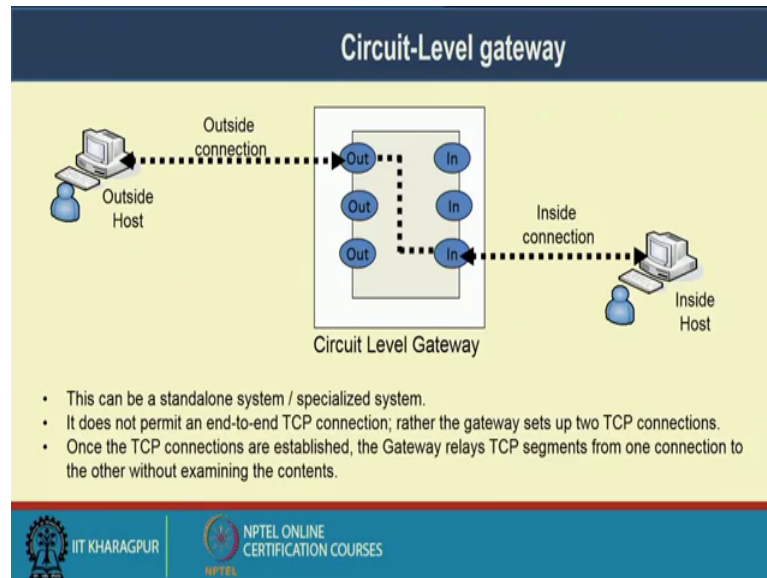
### Application-level Gateway (contd.)

- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic
- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as a choke point)

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

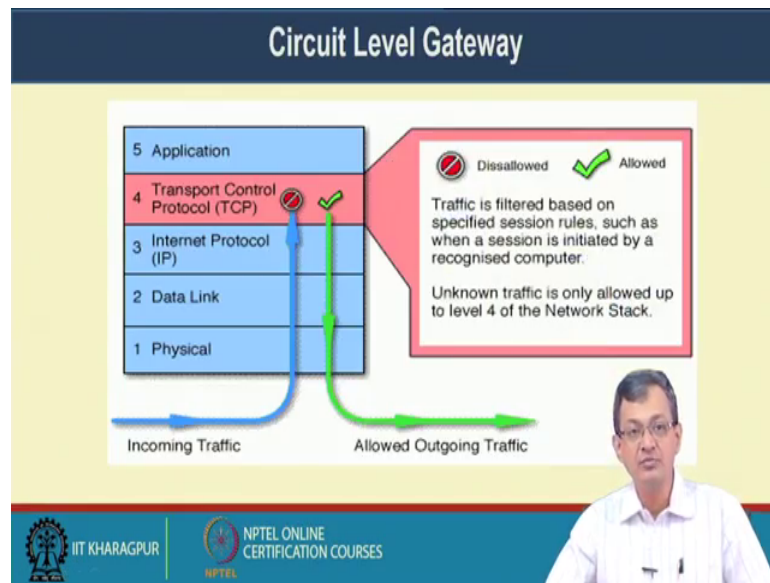
So, application level firewall also proxy server or proxy firewall relay of application traffic access (Refer Time: 25:50) advantages, higher security than packet filters only need to scrutinize a few allowable applications easy to log and audit all incoming traffic right. So, disadvantages additional processing overhead on connection gateway as its spy point etcetera. So, that is the more application more processing things are required.

(Refer Slide Time: 26:13)



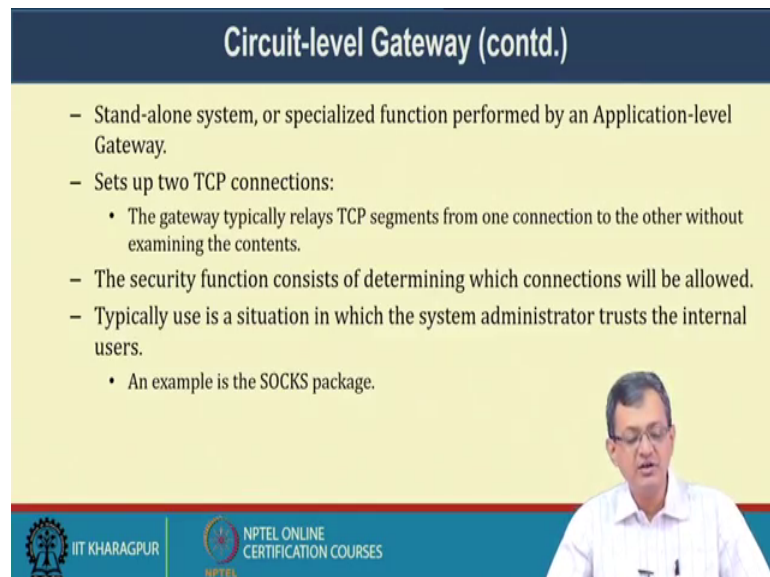
There is another type of things circuit level gateway. So, may not be very popular; popular in the sense we may not be seen this very everywhere, but that there is a thing this can be a standalone system or specialized system. So, it does not permit an end to end TCP connections right; so, usually TCP connections are end to end phenomena. So, this circuit level gateway it does not permit TCP connection rather gateway sets up 2 TCP connections; once the TCP connection are established, the gateway relays TCP segment from one connection to the other without examining the contents. So, that is it breaks the things and create a connection like this so, that it moves like that.

(Refer Slide Time: 27:01)



So, it is again it acts at a transport layer; traffic is filtered based on the specific session rules such as when a session is initiated or by a recognised computer and type of things; so, based on that TCP session. So, as it is a phenomena of the transport layer it is mostly controlled by the transport layer.

(Refer Slide Time: 27:23)






So, stand alone system set up 2 TCP connection; security function consists of determining which connections will be allowed. Typically use situation in which system administrator trusts the internal user; so this socks package is one of such example.

(Refer Slide Time: 27:39)

### Firewall Configurations

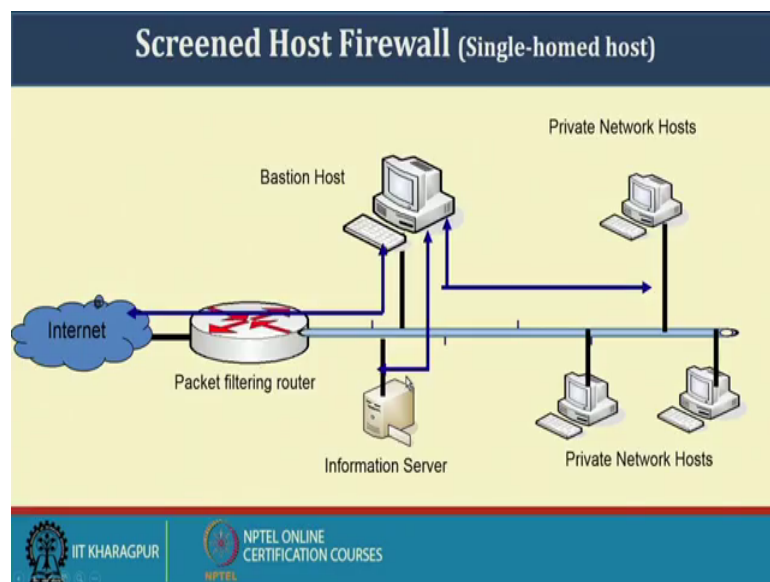
- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible
- Three common configurations are in popular use.



Now regarding firewall configuration in addition to use simple configuration of a single system, more complex configurations are possible 3 common there are very popular uses.

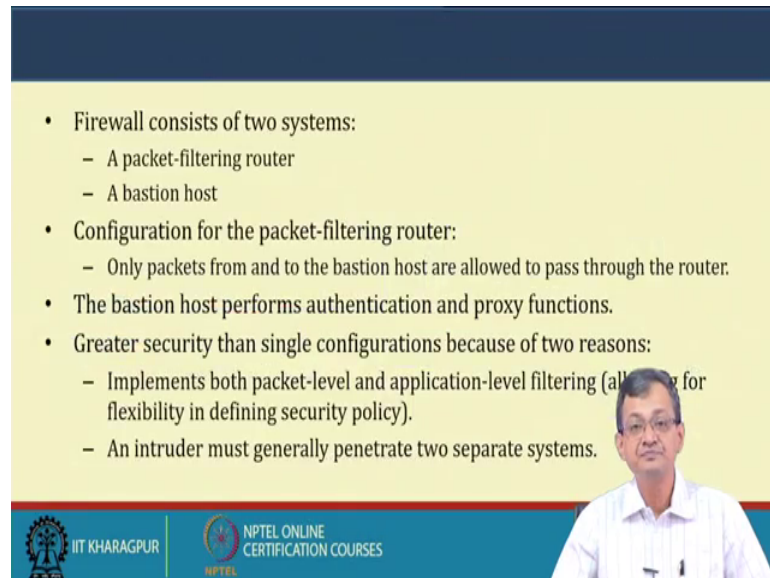
(Refer Slide Time: 27:55)



So, one is the screened firewall like here the traffic comes and then it goes to this packet filtering router and goes to the things right. So, the traffic is connection like this sorry; so, there is a bastion host which is more controlled system the controlled host; where the services which are only needed are enabled the it goes to that traffic for filtering there is

a information server which says that what sort of security filtering or security feature needs to be energized.

(Refer Slide Time: 28:39)



The slide contains a list of bullet points describing a firewall system. A small video inset of a man in a white shirt is visible in the bottom right corner of the slide area.

- Firewall consists of two systems:
  - A packet-filtering router
  - A bastion host
- Configuration for the packet-filtering router:
  - Only packets from and to the bastion host are allowed to pass through the router.
- The bastion host performs authentication and proxy functions.
- Greater security than single configurations because of two reasons:
  - Implements both packet-level and application-level filtering (allowing for flexibility in defining security policy).
  - An intruder must generally penetrate two separate systems.

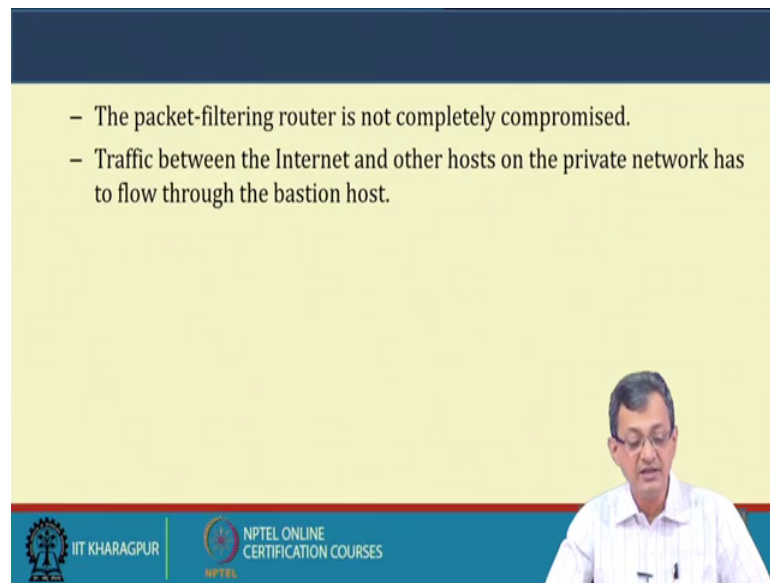
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, as we have seen that it consists of 2 system one is the packet filtering router and the bastion host and the bastion host perform authentication and the proxy function. The greater security than single configuration because of 2 reason implements both packet filter and application filter filtering intruder must generally penetrate to systems to and to compromise the firewall.

So, other one is a screened host firewall dual homed; so, the configuration physically prevents security breach right here the breach is there. So, it goes there and it goes to be there; so it is a physically it is not logically forwarding the packet it is physically protects the things.

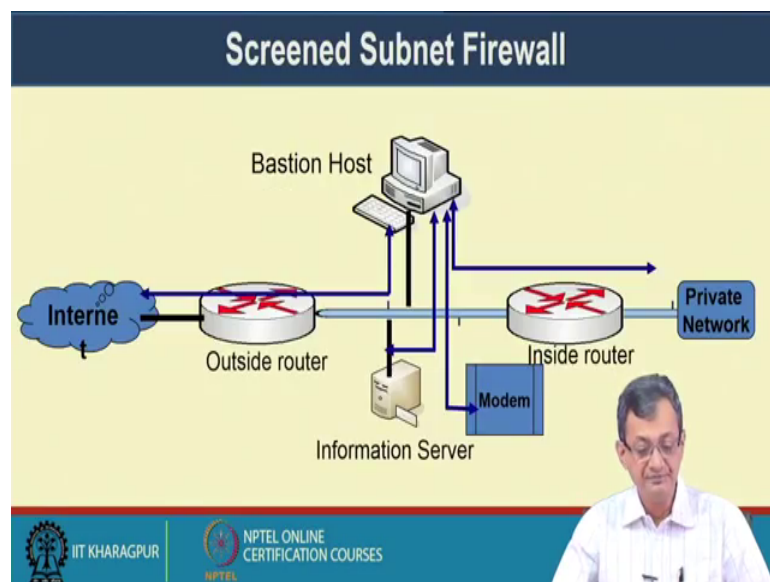
(Refer Slide Time: 29:25)

- The packet-filtering router is not completely compromised.
- Traffic between the Internet and other hosts on the private network has to flow through the bastion host.



And the packet filtering router is not completely compromised and traffic between the internet and other host on the private network as to flow through the bastion host cannot avoid that things; so, that is the way it looks that.

(Refer Slide Time: 29:43)



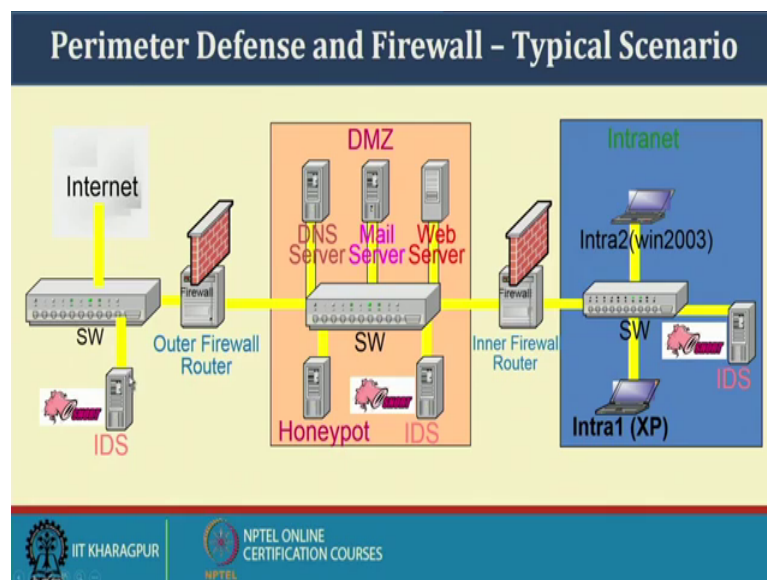
And another is the screened subnet firewall where there we have another internal router so; that means, dual home things are there. So, it is a private and a this is the external and this is the internal router so; that means, 2 layer protection is there. So, a screened



subnet; so I can have now 3 domain right one is the external one is the intermediate and in the another is the on the private network or the internal network on the things right.

This helps us in keeping several servers like say DMZ zone etcetera can be created out here right which need not only goes through these outer firewall; also while connecting to the internal thing has to be connect has to be goes to a internal firewall. So, this is a this is a much better configuration, but as we see that it requires more hardware specification and more configuration issues and increases the host cost and management of the whole system.

(Refer Slide Time: 30:51)



And finally, if we try to look at a typical scenario that what today's systems tries to do. One side is that internet connectivity with a ideas that is your intruder detection systems. Another side is the internal network where things are; there are 2 firewall outer firewall and inner firewall in between there are several things. One the things one the things which are should be in the DMZ row like DNS server, mail server, web server or any other server with that DM zone.

It also has a intrusion detection things which are which could have compromise these or pass this, but there is a intrusion detection based on the whatever it receive in the switch. There is a honey pot as we discussed sometime back; so that it is a where you are expecting latex and learn the signatures of the things. So, this is in the DMZ zone and then we have this inner firewall for the external connectivity.

So, with this let us conclude our discussion on this network security. As I mentioned the network security per se is not part a core part of the course. So, may not be important for your exam point of view, but it is a important for our networking concepts or look means or for practical implementation on it. So, that is why we thought that we should have couple of lectures on the network security to give you some the pointers. Because this is much deep into the things every subject some pointers those who are interested can go into the things. So, as this is the last lecture of our series of courses.

So, first of all let me thank you that you have taken up this course. So, what we tried that too look at different aspects of the computer networks and internet protocols at layer wise. We followed a top down approach starting from the application and going coming down the things and I tried to see that important factor at a different level. Nevertheless to say that is there are lot of things which are still need to be explored what we believe that this will give you a means as I was mentioning some pointers to look into different aspects of the things.

And all with these days several simulators etcetera available and also some many of you having some practical implementation at your workplace or college and type of things. So, it will be nice to explore some of the things, but be careful that you should not do something which bring harm to the network because after all we make this network to have resources shared and able to work together or have that more accessibility to the resource.

So, with this let us conclude this today's talk and also let me thank you again for the taking up this course.

Thank you.