

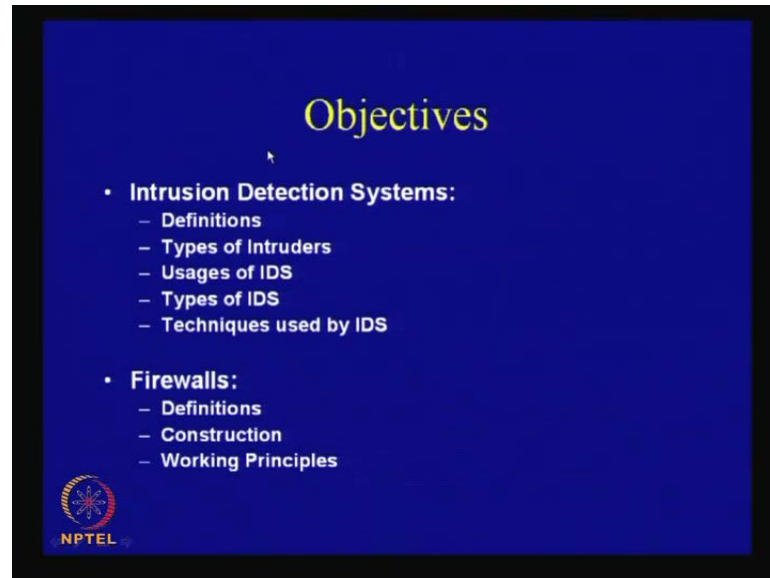
**Cryptography and Network Security**  
**Prof. D. Mukhopadhyay**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Module No. # 01**  
**Lecture No. # 40**  
**Firewalls and Intrusion Detection Systems**

(Refer Slide Time: 00:22)




(Refer Slide Time: 00:29)



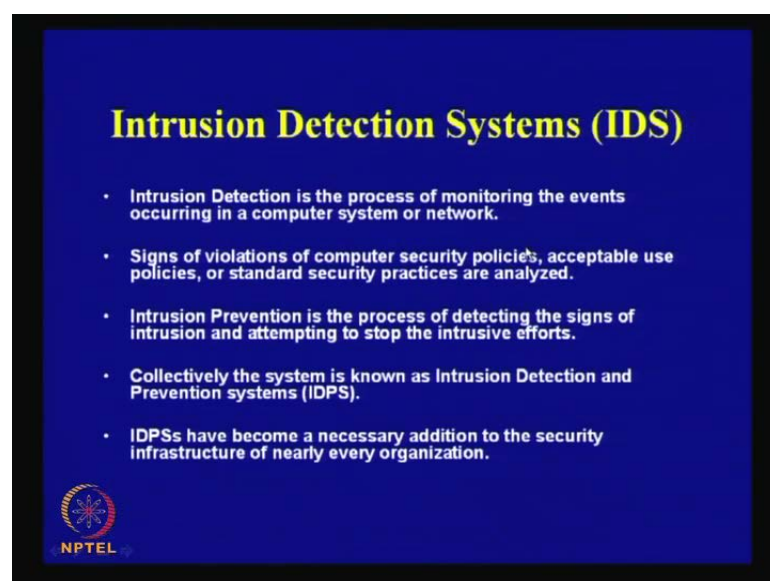
**Objectives**

- **Intrusion Detection Systems:**
  - Definitions
  - Types of Intruders
  - Usages of IDS
  - Types of IDS
  - Techniques used by IDS
- **Firewalls:**
  - Definitions
  - Construction
  - Working Principles

 NPTEL


So, in today's class we shall discuss about firewalls and intrusion detection systems, and so essentially today's topic of discussions will be, we shall actually first discuss about intrusion detection systems. We shall consider the definitions, types of intruders, category of intruders, and also what are the functionalities of intrusion detection systems, and see some of the techniques which are used by these kinds of systems to essentially observe the vulnerabilities or the threats to networks.

(Refer Slide Time: 01:04)



**Intrusion Detection Systems (IDS)**

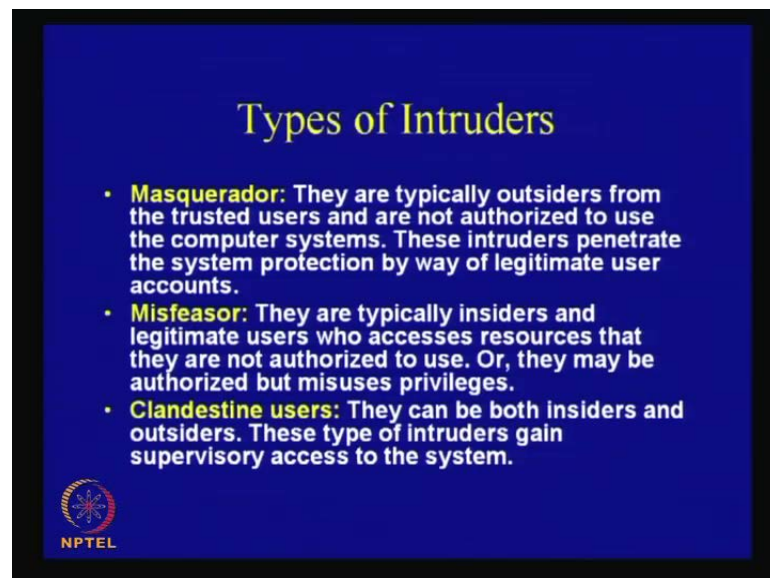
- **Intrusion Detection** is the process of monitoring the events occurring in a computer system or network.
- Signs of violations of computer security policies, acceptable use policies, or standard security practices are analyzed.
- **Intrusion Prevention** is the process of detecting the signs of intrusion and attempting to stop the intrusive efforts.
- Collectively the system is known as **Intrusion Detection and Prevention systems (IDPS)**.
- IDPSs have become a necessary addition to the security infrastructure of nearly every organization.

 NPTEL

Then, we shall discuss important topic about firewalls; consider the definitions constructions, and discuss about the principles which are used behind firewalls. So, intrusion detection system is essentially the process of monitoring the events which occurred in a computer system or networks. Now, signs of violations of computer security policies essentially which are standards security practices are observed by the intrusion detection systems. The intrusion detection systems observe for any possible violations of what are thought to be secured practices.

Now, there are essentially two important broad categories of the intrusion detection system, as such one is called the intrusion detection system and the other one is called the intrusion detection and prevention system. So there are essentially two parts, and it is probably difficult to exactly draw a line between them. So while one concentrates in finding out or detects the security breaches, the other actually prevents or blocks any threats.

(Refer Slide Time: 02:13)



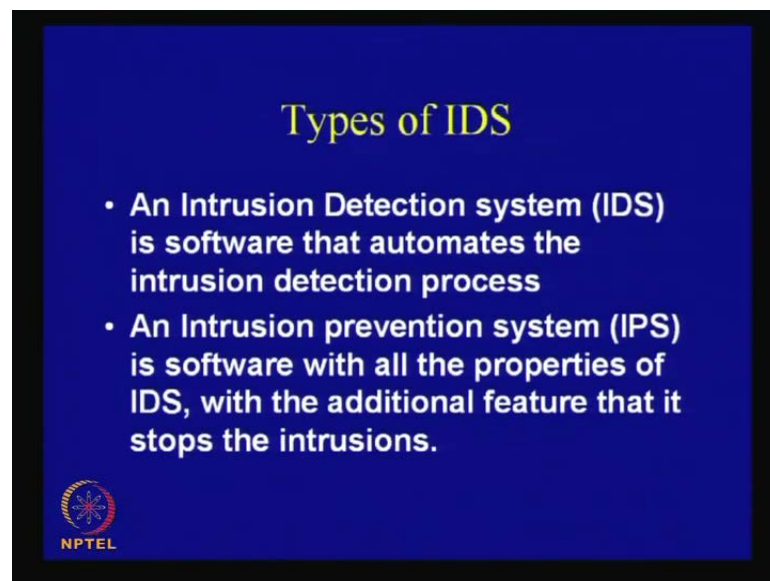
So, an IDPS's as it is collectively called, became a very necessary addition to the security infrastructure of nearly every organization. So looking into this little bit, we shall actually see like for example, there are three types of intruders. So intruders are probably categorized as masqueradors, misfeasors, and clandestine users. Masqueradors are typically outsiders from the trusted users; I am not authorized to use the computer systems, so they generally penetrate the system by essentially some legitimate user

account. Basically, it is kind of like as we have seen in the last class, masquerading attacks in network protocols. So it is like, you try these kinds of attackers, try to mimic or imitate a legitimate user, and create (()), create attacks in the network.

While in the other hand, the misfeasor is typical insider and legitimate user, who actually have got accesses of resources. But the thing is that although they are legitimate users, they are essentially accessing resources which they are not authorized to use. So essentially you can say that, they violate or misuse the privileges that they are provided with.

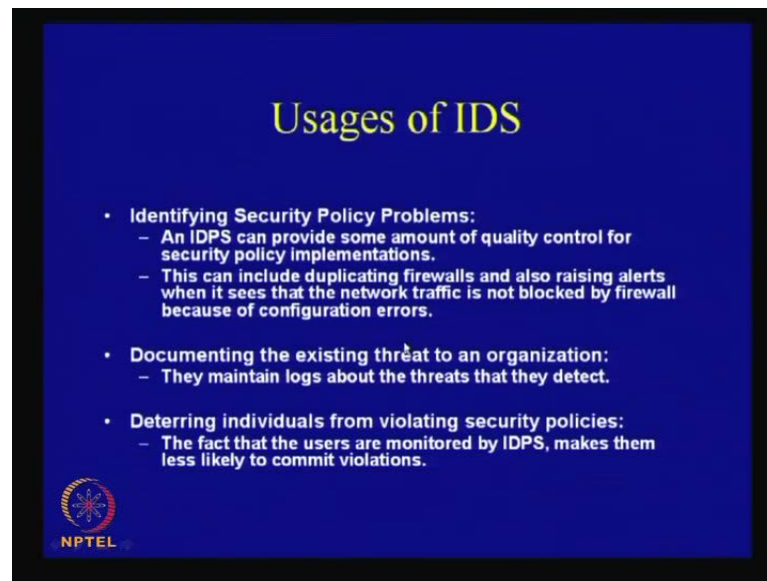
And the third kind of intruders is known as clandestine users. They can be both insiders and outsiders, and these types of intruders typically gain supervisory access to the system. So these are the broad three categories of intruders.

(Refer Slide Time: 03:31)



Now, as we have told that the intrusion detection system can actually be categorized into IDS and IPS, which is the intrusion detection system and the intrusion prevention system. While first, actually concentrate or automates the intrusion detection process, the second one has an additional feature that is it also tries to stop the intrusions.

(Refer Slide Time: 03:51)

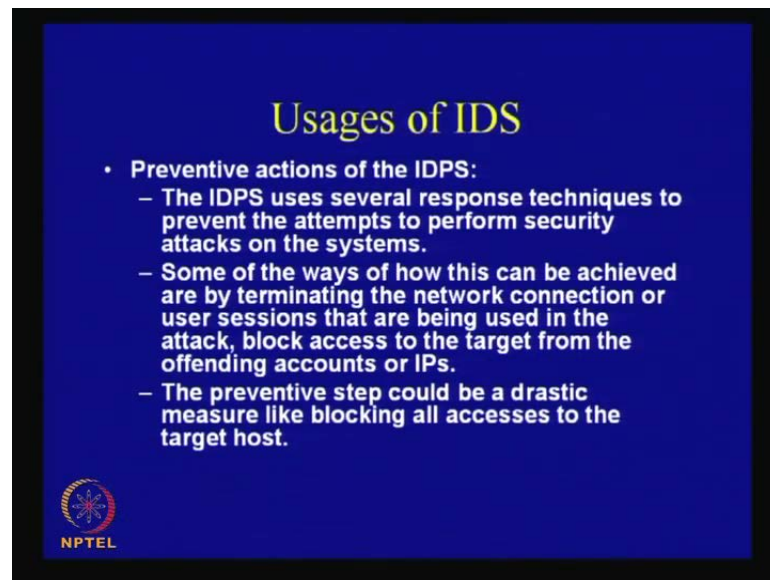


So, we shall actually go into little bit depth since, first of all we shall actually consider some of the uses of IDS's. As we have seen that IDS's; the normal uses of IDS's are essentially in monitoring the network and look for vulnerabilities, and also on the other hand to take some actions to prevent those attacks. But along with it we also have got some other functionalities like, they do some amount of quality control in which they actually not only, I mean they continuously check that whether your security policies which are in place are correct or not. So they may take some steps, like if there are some incorrect settings to your firewalls they will do those corrections. They will raise alerts, whenever it sees that the network traffic is actually not blocking some traffic because of configuration errors.

So, basically it is kind of dials or quality control of the security policies which enforced the implementation and security policies, and along with it very important functionality is to document the existing threat to an organization that is maintain logs about the threat that they detect. So later on, if there be some attacks people can revert back refer to these logs and can actually see what gone into the network. The other important functionality is like since IDPS are placed it generally deters individuals from violating security policies. So it is something like as we know that in shops if there are some CCT cameras, then the thieves are generally **they essentially probably as** more scared to do some criminal activities. So it is something like if we know that we continuously being


monitored, the users know that they are be monitored by IDPS's makes them less likely to commit violations.

(Refer Slide Time: 05:42)



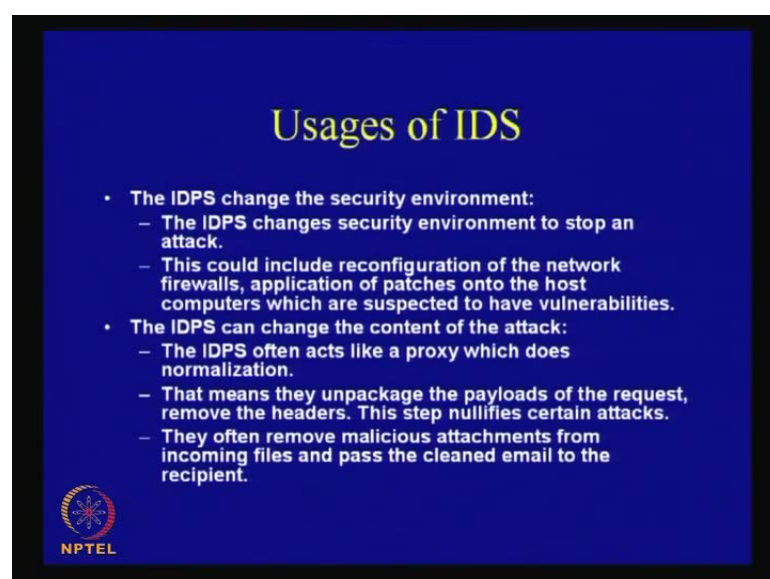
**Usages of IDS**

- Preventive actions of the IDPS:
  - The IDPS uses several response techniques to prevent the attempts to perform security attacks on the systems.
  - Some of the ways of how this can be achieved are by terminating the network connection or user sessions that are being used in the attack, block access to the target from the offending accounts or IPs.
  - The preventive step could be a drastic measure like blocking all accesses to the target host.

 NPTEL


So this is a kind of a functionality which the ideas also performs along with it **also of course definitely performs the** preventive actions, and it essentially adopts several responsive techniques. So responsive techniques could be like from simply identifying that, which network connections or which users sessions are creating threats, and to block them or could be a drastic measure like, even blocking all accesses to a target host.

(Refer Slide Time: 06:11)



**Usages of IDS**

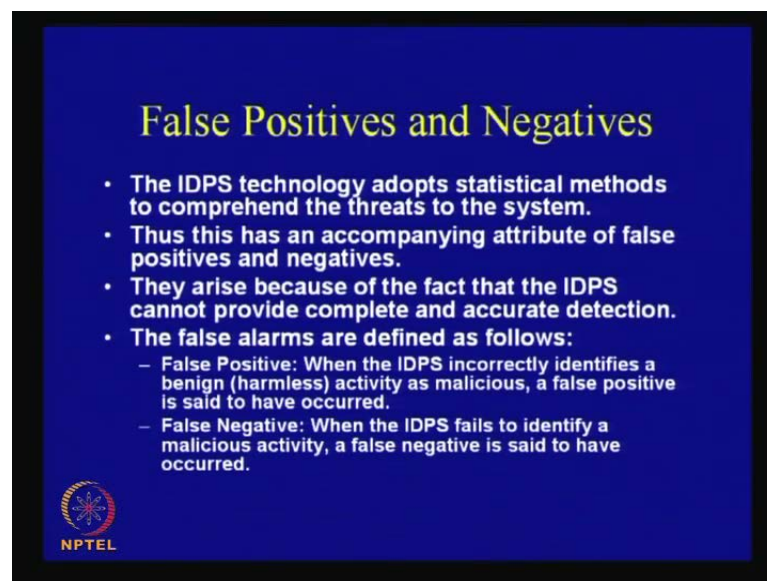
- The IDPS change the security environment:
  - The IDPS changes security environment to stop an attack.
  - This could include reconfiguration of the network firewalls, application of patches onto the host computers which are suspected to have vulnerabilities.
- The IDPS can change the content of the attack:
  - The IDPS often acts like a proxy which does normalization.
  - That means they unpackage the payloads of the request, remove the headers. This step nullifies certain attacks.
  - They often remove malicious attachments from incoming files and pass the cleaned email to the recipient.

 NPTEL




So depending upon your security measurement, the IDS take its preventive actions. Now the IDS's the IDPS's also changes the security environments which means that it will change the security environment to stop an attack, and this could actually include reconfiguration of the network firewalls application of patches. As we have seen in the last class like, if there are some vulnerabilities detected in the system then it is also important to update the patches. So the IDPS also does this functionality of updating the patches which are suspected to have vulnerabilities. Along with it, it also does some amount of normalization which means that if the payload of the network traffic contains some suspected headers then they are removed. These actually helps to prevent some kind of attacks, and they also often remove the malicious attachments from incoming files and pass that clean email to the recipient. So, this is also some important functionality which the IDS perform.

(Refer Slide Time: 07:04)



**False Positives and Negatives**

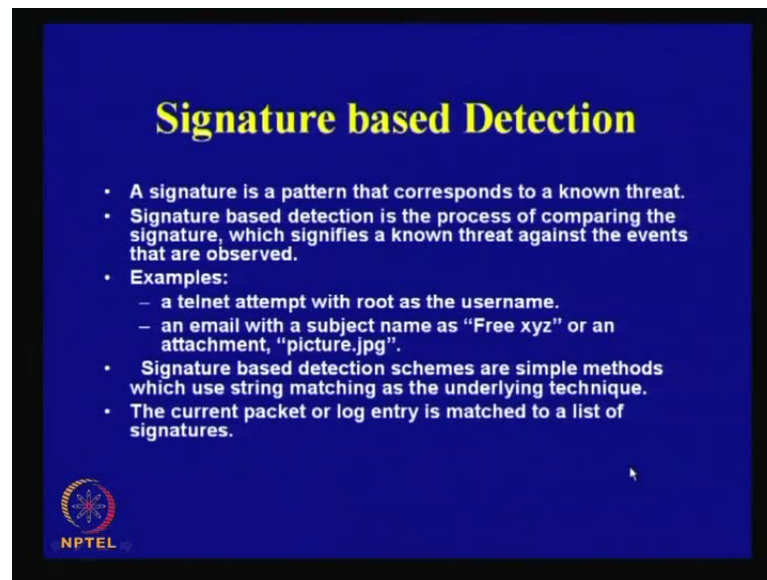
- The IDPS technology adopts statistical methods to comprehend the threats to the system.
- Thus this has an accompanying attribute of false positives and negatives.
- They arise because of the fact that the IDPS cannot provide complete and accurate detection.
- The false alarms are defined as follows:
  - False Positive: When the IDPS incorrectly identifies a benign (harmless) activity as malicious, a false positive is said to have occurred.
  - False Negative: When the IDPS fails to identify a malicious activity, a false negative is said to have occurred.

 NPTEL

Now, since the IDPS technology actually adapts statistical methods to comprehend the threats to the system, so they have some accompanying attribute of false positives and false negatives which comes with any statistical measure. So as we know that false positive indicate that the IDPS actually incorrectly identifies **or suppose only** harmless activity as malicious and false negative. On the other hand, when an IDPS fails to identify a malicious activity, we immediately understand that the false negative is something which is probably more threatening. Therefore, the first objective will be to prevent or reduce the false negatives, and then if they have some false positives which

comes along with it then additional measures can be taken to really understand whether the detected packets are really harmful or not.

(Refer Slide Time: 07:54)

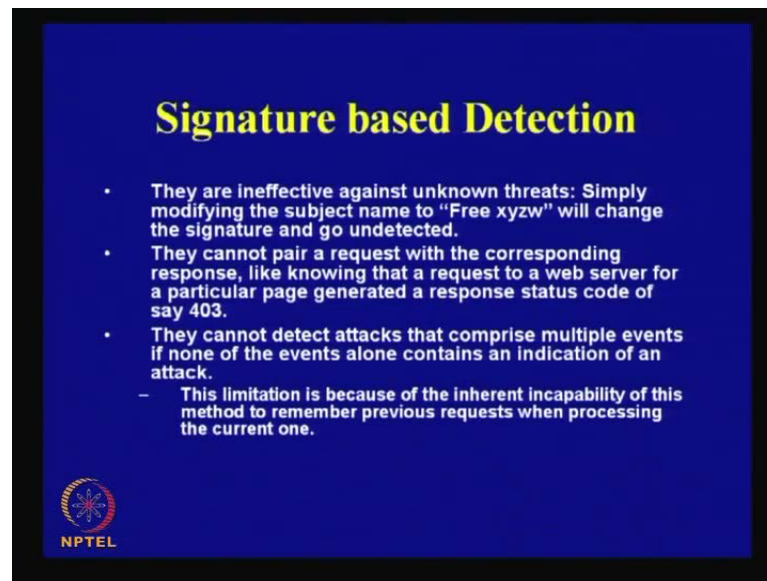


So, there are various detection methods which are followed by IDPS's, one of the most whether known techniques or whether most primitive technique would be a signature based intrusion detection system. So in this, signature is essentially defined as a pattern that corresponds to a known threat. Signature based detection is the process of comparing the signatures which signifies a known threat against the events that are observed. So examples could be like for example, there is a telnet attempt made with root as a username, so this is a typical example which is generally prevented by IDPS's.

The other thing could be like if there are some attachments which are suspected, then the IDPS actually does the normalization activity and remove these attachments. But then these are extremely simple methods that actually can use string matching techniques as the underlying principles, and the idea is that the current packet or the log entry is matched to the list of signatures and if the match is found those packets have locked or stopped.




(Refer Slide Time: 09:03)



**Signature based Detection**

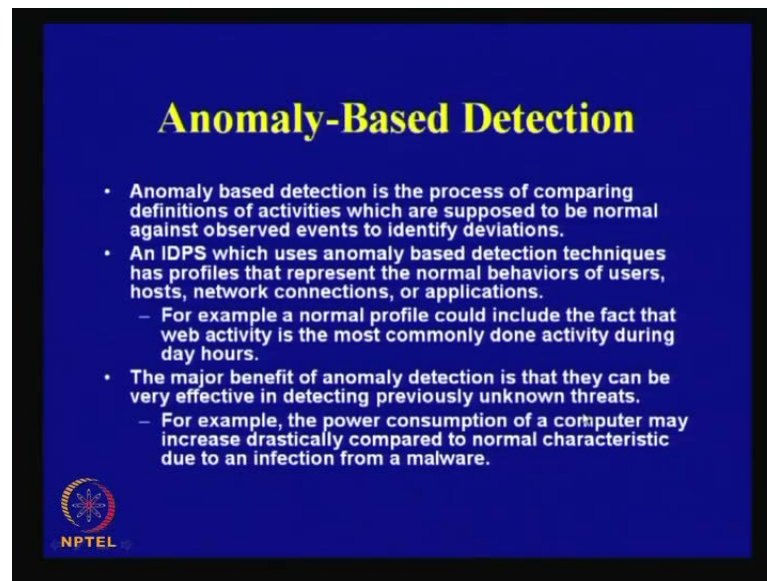
- They are ineffective against unknown threats: Simply modifying the subject name to "Free xyzw" will change the signature and go undetected.
- They cannot pair a request with the corresponding response, like knowing that a request to a web server for a particular page generated a response status code of say 403.
- They cannot detect attacks that comprise multiple events if none of the events alone contains an indication of an attack.
  - This limitation is because of the inherent incapability of this method to remember previous requests when processing the current one.

  
NPTEL

Now this being a very simple technique, of course it is ineffective against unknown threats for example, simply someone can modify the name of the subject or may modify the name of the attachments and can go undetected. So they cannot, the other bad point about these kind of techniques is that they cannot pair a request with a corresponding response like it cannot say for example, 403 which is, I mean error status code which is a prohibited website that has been accessed. So, it cannot pair to the corresponding request which has been made. This incapability of remembering previous requests when possessing the current one makes it like that. This kind of detection schemes cannot detect attacks that comprise multiple events that means if an attack is built out of actually multiple events then these kind of signatures schemes cannot prevent them.


As it cannot actually pair the previous requests with the current one; I mean you cannot remember a history of the requests or the responses, therefore these are incapable of preventing attacks which comprise of multiple events.

(Refer Slide Time: 10:30)



**Anomaly-Based Detection**

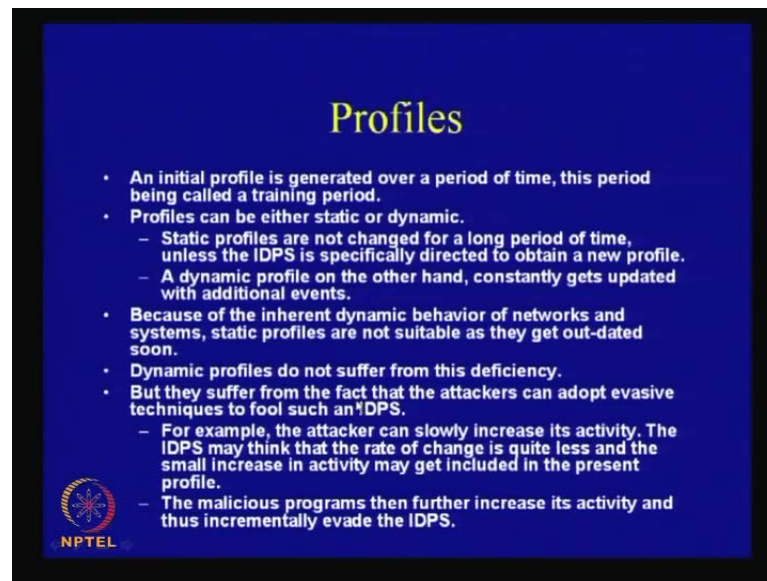
- Anomaly based detection is the process of comparing definitions of activities which are supposed to be normal against observed events to identify deviations.
- An IDPS which uses anomaly based detection techniques has profiles that represent the normal behaviors of users, hosts, network connections, or applications.
  - For example a normal profile could include the fact that web activity is the most commonly done activity during day hours.
- The major benefit of anomaly detection is that they can be very effective in detecting previously unknown threats.
  - For example, the power consumption of a computer may increase drastically compared to normal characteristic due to an infection from a malware.

  
NPTEL

So, the other important detection scheme which is known as the anomaly based detection scheme **now these detection schemes** are actually based on the process of comparing definitions of activities which are supposed to be normal against observed events to identify deviations. So an IDPS which uses anomaly based detection schemes **so essentially it** generally builds up profiles like it builds up the profiles for the normal behaviours of the user's hosts or network connections or applications and it matches the present activities with those profiles. Now the important advantage that one can derive out of anomaly based detection systems is that, it can be used to detect previously unknown threats. So for example, the system could be based like if there is a malicious activity; suppose a profile is built out to essentially capture the power consumption of the of the device, so the idea is that if there has been some infection from a malware then the power consumption of the device can increase. Such kind of detection scheme helps because of the fact that, although your malwares can vary it can come from unknown malware.


But that technique of detection is through a means which is actually immaterial or does not really depend on the exact mode or form of attack. For example, it does not actually depend upon which malware is attacking because the signature is something which is quite common, and general like the power consumption of the computer.

(Refer Slide Time: 12:16)



## Profiles

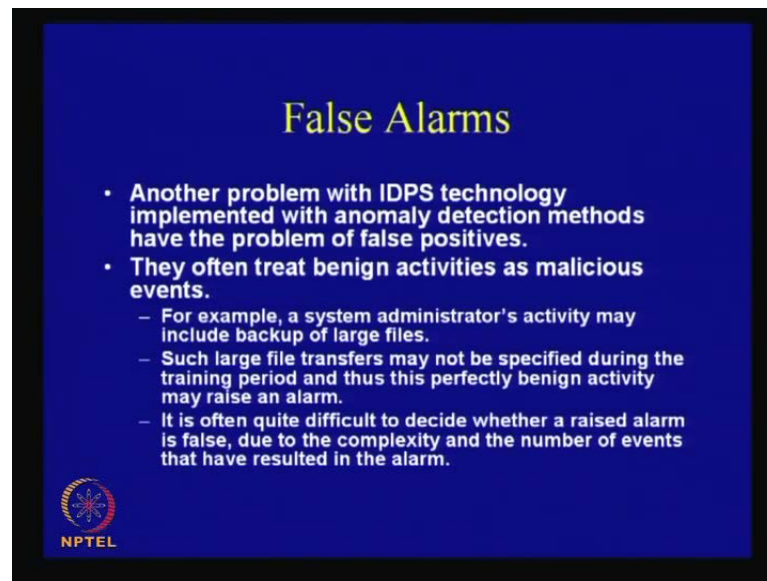
- An initial profile is generated over a period of time, this period being called a training period.
- Profiles can be either static or dynamic.
  - Static profiles are not changed for a long period of time, unless the IDPS is specifically directed to obtain a new profile.
  - A dynamic profile on the other hand, constantly gets updated with additional events.
- Because of the inherent dynamic behavior of networks and systems, static profiles are not suitable as they get out-dated soon.
- Dynamic profiles do not suffer from this deficiency.
- But they suffer from the fact that the attackers can adopt evasive techniques to fool such an IDPS.
  - For example, the attacker can slowly increase its activity. The IDPS may think that the rate of change is quite less and the small increase in activity may get included in the present profile.
  - The malicious programs then further increase its activity and thus incrementally evade the IDPS.

 NPTEL

So this actually helps to or other can be very effective in detecting previously unknown threats. Therefore, talking about profiles there are generally two ways in which a profile is built, one is called the static profiles and another one is called the dynamic profiles. Now, static profiles are generally not changed for a long period of time until the IDPS specifically tells it to change it, while on the other hand, the dynamic profile continuously updates with the additional events. Now it has been understood easily that because of the event dynamic behaviour of the networks and systems, if you maintain a static profile then it will get outdated very soon.


On the other hand, dynamic profiles actually do not suffer from this deficiency, but dynamics profiles also **there is a kind of that is** have a weak point that they can actually use by attackers to fool an IDPS. The thing is that for example, an attacker can slowly increase his activity, and initially the IDPS can think that the rate of increase is not allowed. And therefore, what it will do is it will add the increased activity into its profile and then, the moment it is added the malicious program can actually further increase its activity. So, in this way it cannot actually incrementally increase its activity, and finally can evade the intrusion detection prevention systems.

(Refer Slide Time: 13:45)



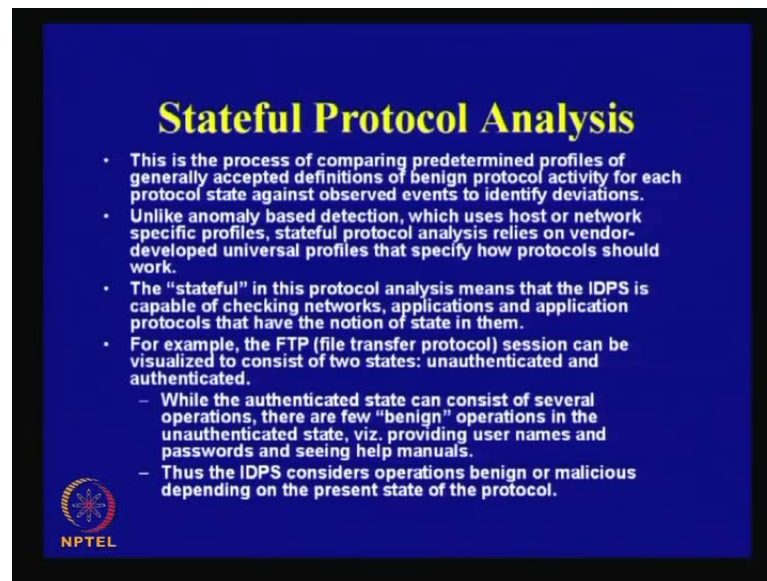
**False Alarms**

- Another problem with IDPS technology implemented with anomaly detection methods have the problem of false positives.
- They often treat benign activities as malicious events.
  - For example, a system administrator's activity may include backup of large files.
  - Such large file transfers may not be specified during the training period and thus this perfectly benign activity may raise an alarm.
  - It is often quite difficult to decide whether a raised alarm is false, due to the complexity and the number of events that have resulted in the alarm.

  
NPTEL


So if you used a profile, it has to be a combination of static profiles as well as dynamic profiles. Now there is another problem with IDPS technology implemented with anomaly detection methods that is, there is a problem of false positives that is they often treat the benign activities as malicious events. For example, system or administrator very typical job could be, to include back up of large files. Now, this could be actually treated as a profile for an attack and therefore, although this is a benign activity and can actually raise false alarms in the network, it is often difficult to decide whether a raised alarm is false due to the complexity and the number of events that are resulted in the alarm. Therefore, this also needs to be kept in mind that anomaly based detection systems can actually come with the problem of false positives.

(Refer Slide Time: 14:34)



**Stateful Protocol Analysis**

- This is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations.
- Unlike anomaly based detection, which uses host or network specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how protocols should work.
- The "stateful" in this protocol analysis means that the IDPS is capable of checking networks, applications and application protocols that have the notion of state in them.
- For example, the FTP (file transfer protocol) session can be visualized to consist of two states: unauthenticated and authenticated.
  - While the authenticated state can consist of several operations, there are few "benign" operations in the unauthenticated state, viz. providing user names and passwords and seeing help manuals.
  - Thus the IDPS considers operations benign or malicious depending on the present state of the protocol.

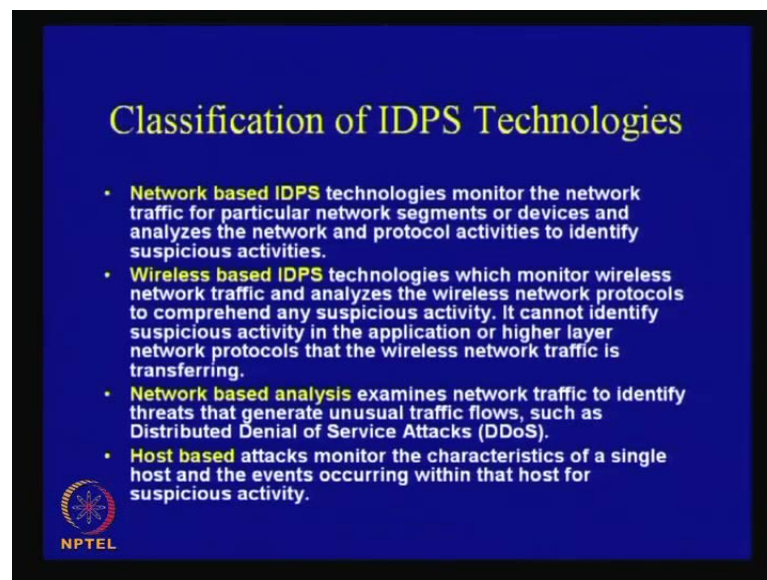
 NPTEL

Now the other important method based on which the intrusion detection systems are built on is something called as the stateful protocol analysis. In this kind of protocol analysis, they often compare predetermined profiles of generally accepted definitions of benign protocols activities for each protocol state against observed events to identify deviations. So the idea is that, this kind of systems also based on the profiles, but the thing is that these profiles are dependent on the states of the protocols therefore, there is a concept of state relevant, and it depends upon the concept of states in the inherent protocol. Now, this is actually the reason why this stateful analysis is often useful because it helps to monitor the security of very common file type of protocols or protocols of this nature which has got inheritance states involved.

Therefore for example, the FTP or the file transfer protocol session can be visualized to consist of two states, so one is the unauthenticated state and the other is the authenticated state. Now in the unauthenticated state, while there are very few operations, **I mean there actually very, there are several operations** there are actually very few benign operations **in the unauthenticated state** for example, like providing user names and passwords and similarly help manuals. Therefore, the IDPS actually considers operations which are benign or malicious depending on the present state of the protocol, therefore this stateful protocol analysis is actually useful because it helps to monitor the security of protocols which are actually have got inherent state in them.


So, another point which needs to be kept in mind is that unlike anomaly based detection schemes which use host or network specific protocols, stateful protocol analysis relies on vendor developed universal profiles that specify how a protocol should work. Therefore, this is actually not dependent on the host or the networks specific profiles, but it is actually specified previously by the vendor. So, whenever a protocol is being developed the vendor actually is essentially specifying what is meant by a benign profile. Therefore, this is very significant difference from the previous **that is the anomaly based detection systems that are the both users profiles**, but there is the difference in the profile which an anomaly based detection system uses and the profile which a stateful protocol analysis uses.

(Refer Slide Time: 17:26)



**Classification of IDPS Technologies**

- **Network based IDPS** technologies monitor the network traffic for particular network segments or devices and analyzes the network and protocol activities to identify suspicious activities.
- **Wireless based IDPS** technologies which monitor wireless network traffic and analyzes the wireless network protocols to comprehend any suspicious activity. It cannot identify suspicious activity in the application or higher layer network protocols that the wireless network traffic is transferring.
- **Network based analysis** examines network traffic to identify threats that generate unusual traffic flows, such as Distributed Denial of Service Attacks (DDoS).
- **Host based** attacks monitor the characteristics of a single host and the events occurring within that host for suspicious activity.

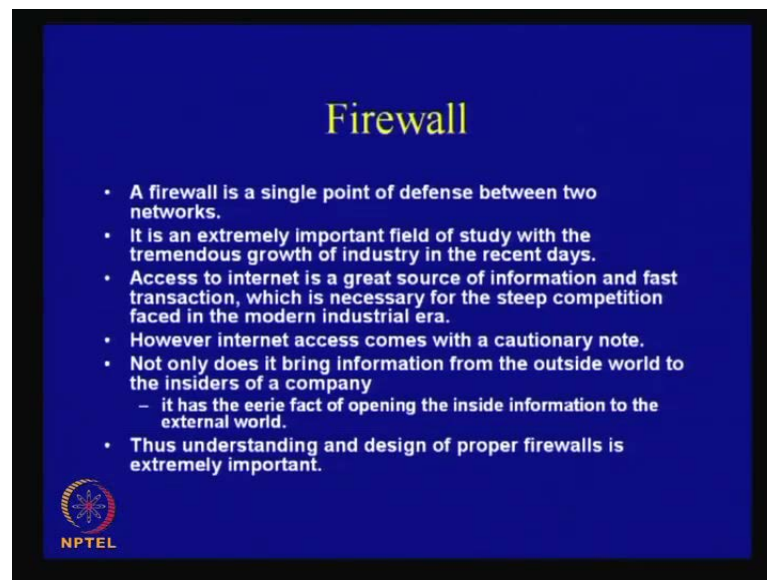
 NPTEL

So that is also a further, I mean as we have seen that based on the prevention techniques you can classify the IDPS technologies. Similarly, you can classify your IDPS technologies depending upon where it is actually used. So, the IDPS technologies often used for the network is known as network based IDPS technologies. They monitor the network traffic for the particular network. And also you can have here wireless based IDPS technologies which monitor the wireless network traffic, analyzes suspicious activities, and looks about the security of wireless networks. You also have your network based analysis which actually examines the network traffic to identify threats that generates unusual traffic flows such as the distributed denials of service attacks or which is probably called as the D DoS attacks.



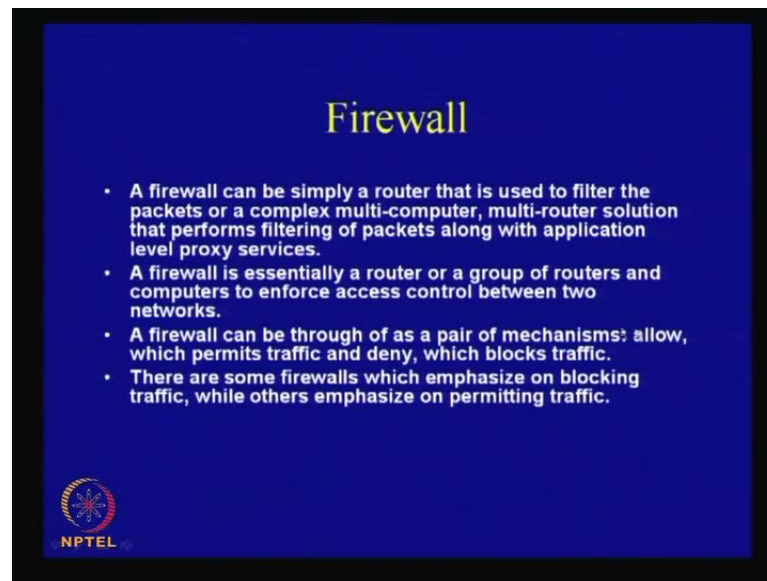
You also have the host based attacks which monitor the characteristics of a single host and the events which occurred within that host for suspicious activity. So depending upon where the IDPS technology has been used, you have got various classifications of the IDPS technology.

(Refer Slide Time: 18:34)



Now, we come into the other part of our discussion which is the firewalls. What is a firewall, so the firewall is essentially a single point of defense between two networks, and is extremely important field of study with the tremendous growth of industry in the recent days. So, the access to internet is a great source of information but of course, it comes with the accompanied problem that you have to ensure that there is really security is maintaining the enterprise. Therefore, all those accesses to internet comes out with a boon; there is an eerie fact of opening of the inside information to the external world. This is actually huge amount of concern for industry because they have got the rights, and another thing which is business secrets is that the entire business can get compromised or hampered.

(Refer Slide Time: 19:34)



Therefore, understanding and designing of proper firewalls is important, and looking into this I mean, the firewall is essentially nothing but router or may be a group of routers or computers which ensures access control between two networks. So, there are two networks which could not trust each other, and a firewall is kind of a guard which switches between them and tries to enforce the mechanisms like access controls between these networks. Typically, the firewall actually uses a pair of mechanisms; it uses a mechanism which is called as allow, which actually permits the traffic, and the other is of course deny which actually blocks the traffic. Now, there are some firewalls which actually emphasize on blockings, while some are not like them, so they essentially emphasizes on actually permitting the traffics.

(Refer Slide Time: 20:21)



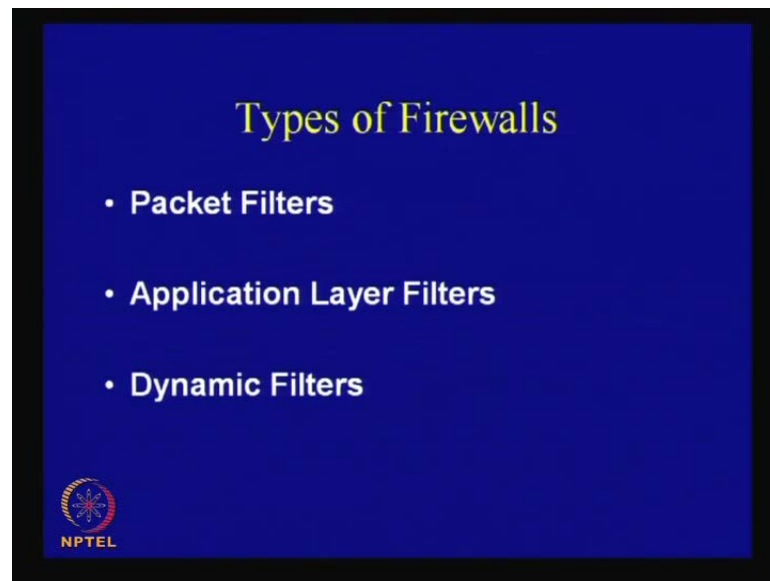
**Firewalls are the guards of our network**

- **Demilitarized Zone (DMZ): Separation between the external perimeter of network and the internal perimeter of network.**
- **Suitable guards are enforced between the Internet and the DMZ and the DMZ and the internal network.**
  - internet to internal network: integrity is issue.
  - internal network to internet: integrity and confidentiality are both issues.
  - these guards are technically known as firewalls.

  
NPTEL

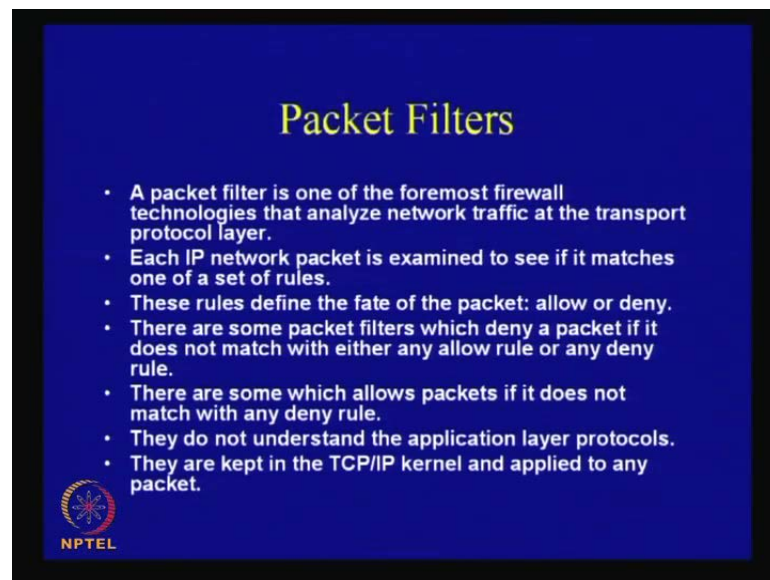
Therefore, a very common name which is known as the demilitarized zone is actually a separation between the external perimeter of a network and the internal perimeter of a network. And the firewalls are essentially is kind of guards which are actually sitting between the internet and the DMZ that is the demilitarized zone, and the DMZ and the internal network. So for example, when you are considering an information exchange from the internet to the internal network, then you are more bothered about the integrity; you are not actually bothered about the confidentiality of the data. But when it is from the other way round that is from the internal network to the internet, you actually bothered not only about the integrity but you also bothered about the confidentiality.

(Refer Slide Time: 21:10)



So, these guards are technically known as the firewalls. Typically, there are three kinds of firewalls which are used, so the three types of firewalls are known as the packet filters, application layer filters, and dynamic filters.

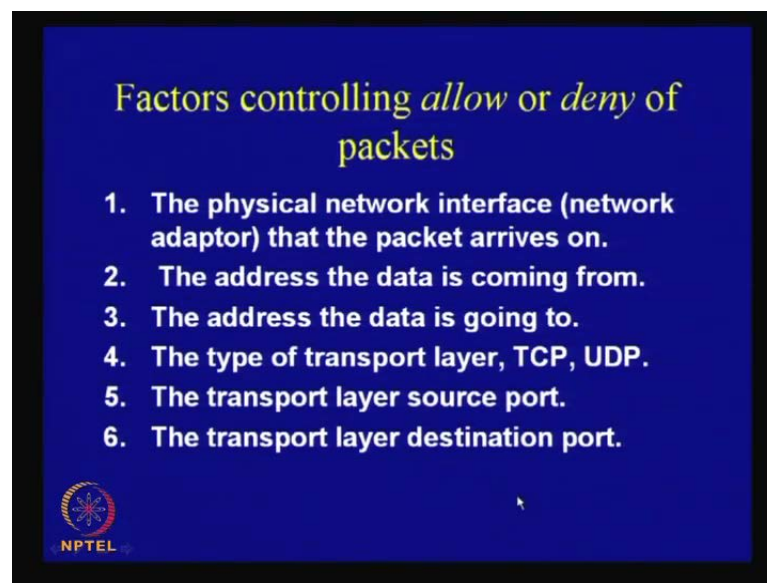
(Refer Slide Time: 21:32)



We will just have a quick look into what are these types of firewalls, and what is the basic principle of working of these firewalls. So, a packet filters are actually the foremost and most primitive technologies that analyze network traffics at the transport protocol layer. Each IP network package is examined to see if it matches a set of rules; these rules

define the fate of the packet that is either it will be allowed or it will be blocked or denied. Now, there are some packets filters which deny a packet if it does not match with either any allow rule or any deny rule. There are some which actually allows packet if it does not match with any deny rule. So, as I told you that your firewalls can actually be more inclined towards blocking or it can be also more inclined towards allowing the packets. So that depend upon the strategy of the network, and they do not actually understand the application layer protocols, so they actually analyze the network traffic at the transport layer protocols. Therefore, the packet layer **seeks** are the transport layer, and it tries that the packet filters analyze the networks at the transport protocol layer and not at the application layer protocols. So, they are typically kept in the TCP IP kernel, and applied to any incoming packet or outgoing packet.

(Refer Slide Time: 22:45)

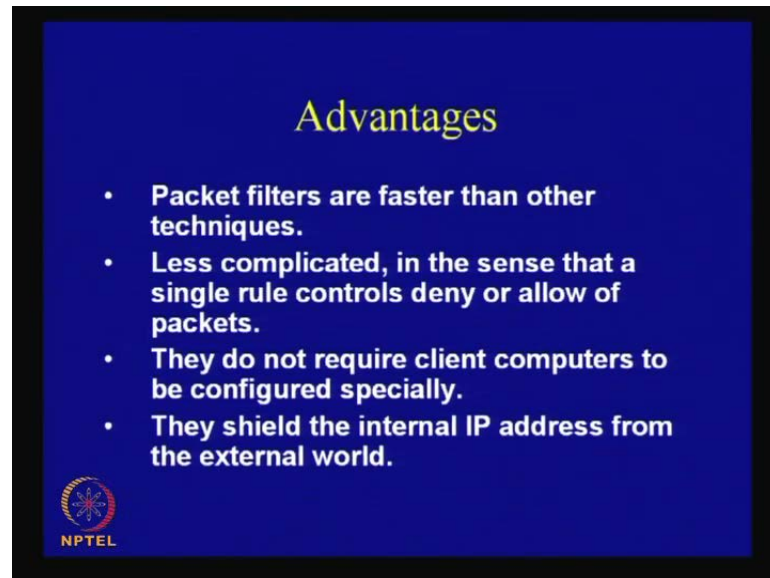


Now, typically the factors which controls the allow or deny of the packets are as follows: the physical network interface or the adapter that the packet arrives on, the address the data is coming from, the address the data is going to, the type of transport layer that is whether it is TCP or whether it is UDP, the transport layer source port, and the transport layer destination port.

So, these are the typical factors which are actually maintained in the allow or the deny rules of the packet filter, and they are checked with the incoming or the outgoing


packets. If they match then they are allowed, if they are not then either they are denied or blocked.

(Refer Slide Time: 23:23)



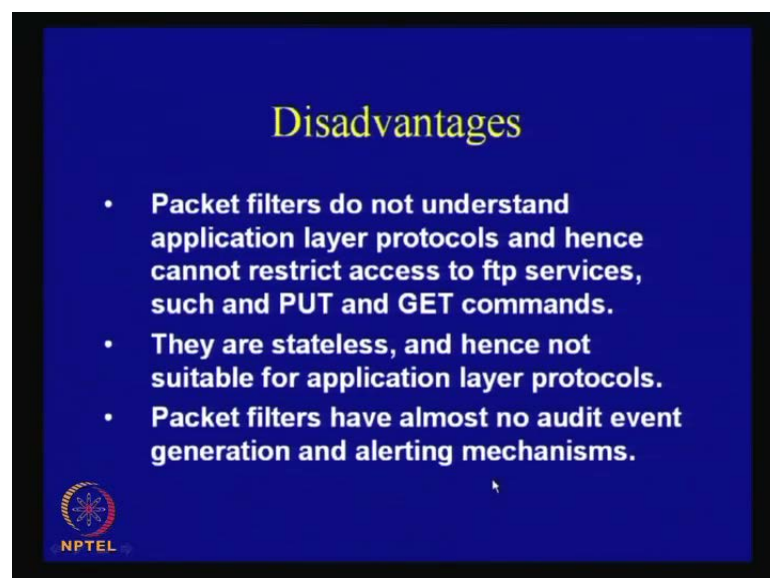
**Advantages**

- **Packet filters are faster than other techniques.**
- **Less complicated, in the sense that a single rule controls deny or allow of packets.**
- **They do not require client computers to be configured specially.**
- **They shield the internal IP address from the external world.**




So, the advantages of the packet filters are, of course they are fast because they do minimize security check, and they are very less complicated. They do not require the client computers to be configured specially, and also they shield the internal IP addresses from the external world. Like you do not see exactly what is the internal IP address of the network when you are communicating with a network in the internal IP'S.

(Refer Slide Time: 23:50)



**Disadvantages**

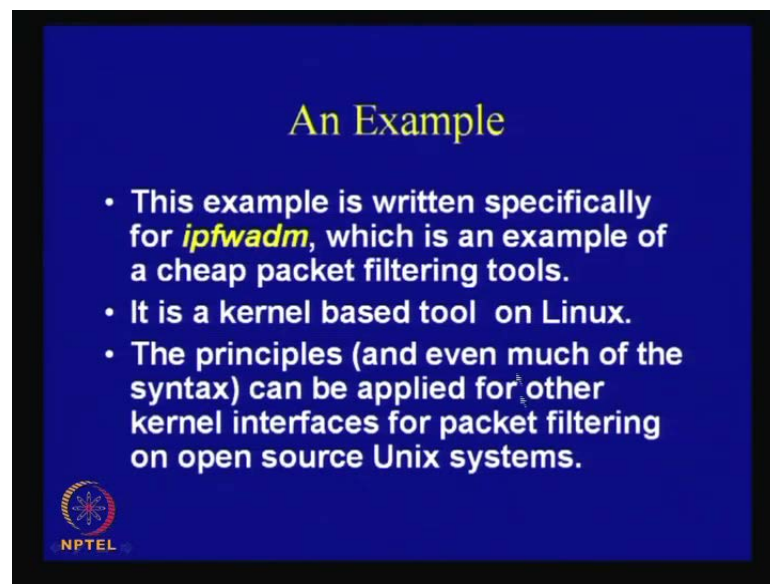
- **Packet filters do not understand application layer protocols and hence cannot restrict access to ftp services, such and PUT and GET commands.**
- **They are stateless, and hence not suitable for application layer protocols.**
- **Packet filters have almost no audit event generation and alerting mechanisms.**





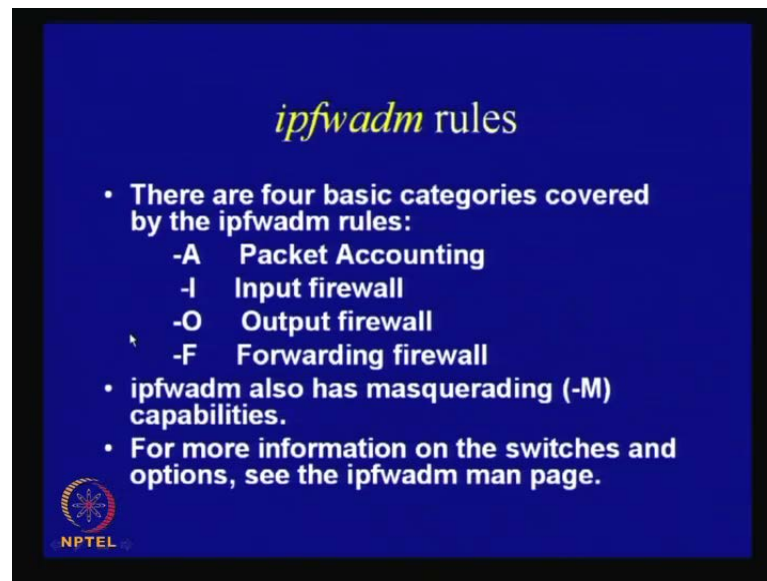
But there are some disadvantages like, they do not understand the application layer protocols, and hence they cannot restrict accesses to the FTP services such as the put and the get commands. They are stateless and hence they are not suitable for the application layer protocols. The packet filters have almost no audit event generation and alerting mechanism, so they do not do proper amount of documentation or do not maintain audits about the network events.

(Refer Slide Time: 24:18)




Now I give a brief example, this example is specifically written for ipfwadm, which is an example of a cheap packet filtering tool, and which is the kernel based tool on Linux. The principles and even much of the syntax can be applied for other kernel interfaces for packet filtering on any open source UNIX systems.

(Refer Slide Time: 24:38)



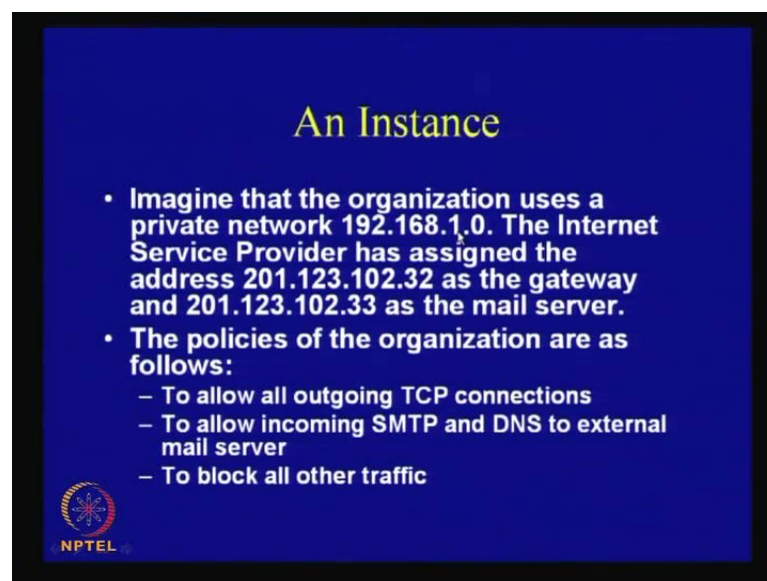
*ipfwadm* rules

- There are four basic categories covered by the ipfwadm rules:
  - A Packet Accounting
  - I Input firewall
  - O Output firewall
  - F Forwarding firewall
- ipfwadm also has masquerading (-M) capabilities.
- For more information on the switches and options, see the ipfwadm man page.




So here is an example, I would not go much but if you do a man of this ipfwadm, then you will see that these are some of the basic switches which you have like the packet accounting, input firewall, output firewall, and the forwarding firewall. There are lots of other switches also, like you can also mention masquerading capabilities. So, for other information on the switches you can actually see the corresponding man page.

(Refer Slide Time: 25:03)



An Instance

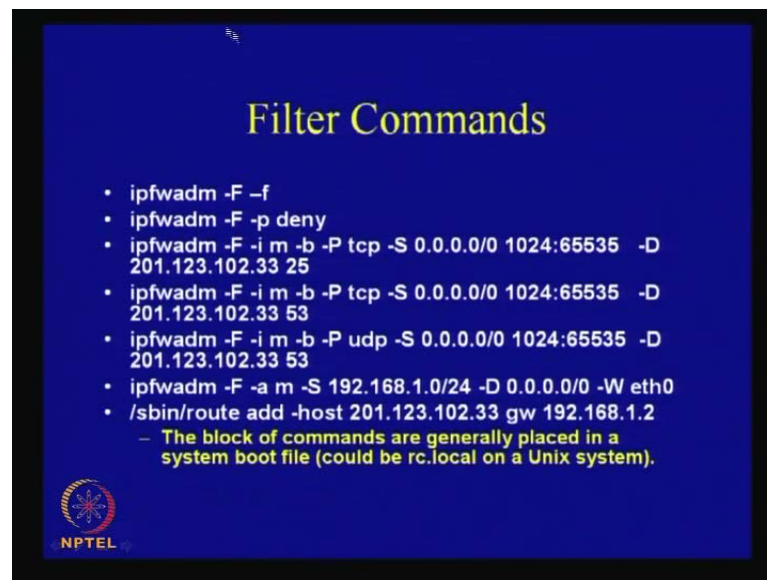
- Imagine that the organization uses a private network 192.168.1.0. The Internet Service Provider has assigned the address 201.123.102.32 as the gateway and 201.123.102.33 as the mail server.
- The policies of the organization are as follows:
  - To allow all outgoing TCP connections
  - To allow incoming SMTP and DNS to external mail server
  - To block all other traffic



Here is an example like, you can imagine that an organization uses a private network, and this is the kind of IP which is provided, and the internet service provider has

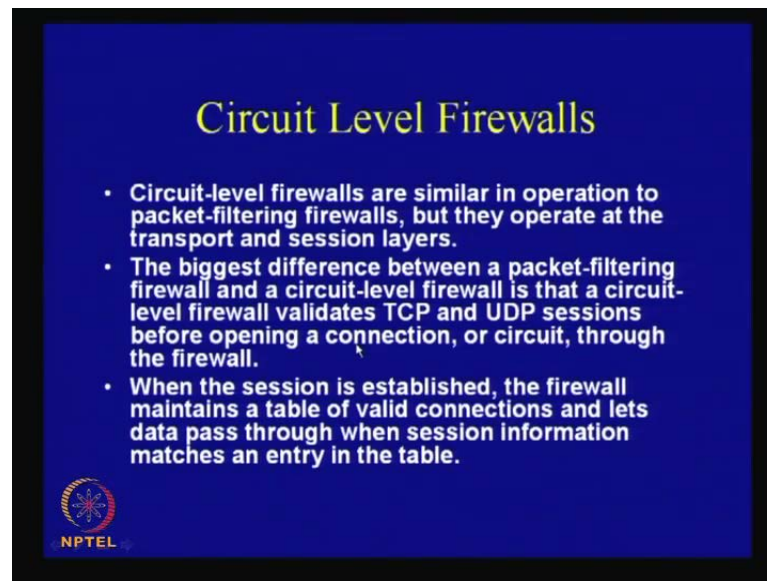
assigned that the address as mentioned here as the gateway, and this as the mail server. So, suppose this is the policy; the policy is like to allow all the outgoing TCP connections, the policy could be to allow incoming SMTP and DNS to external mail server, and it could be to block all other traffics.

(Refer Slide Time: 25:31)




Therefore, depending upon the policies different kind of rules are set like for example, these are the some of the commands which have been provided here. So, these block of commands are generally placed in a system boot file, therefore it could be like an r c dot local on a Unix system and these are kind of executed. You can see like, there are various features like forwarding, denying, which particular IP is being denied. You can also have your masquerading capabilities, and therefore these are the basic rules which are set by using this ipfwadm command. Now, whenever an incoming packet and outgoing packet comes in, then these will be checked against these rule, and depending upon these rules they will be either allowed or they will be denied.

(Refer Slide Time: 26:20)



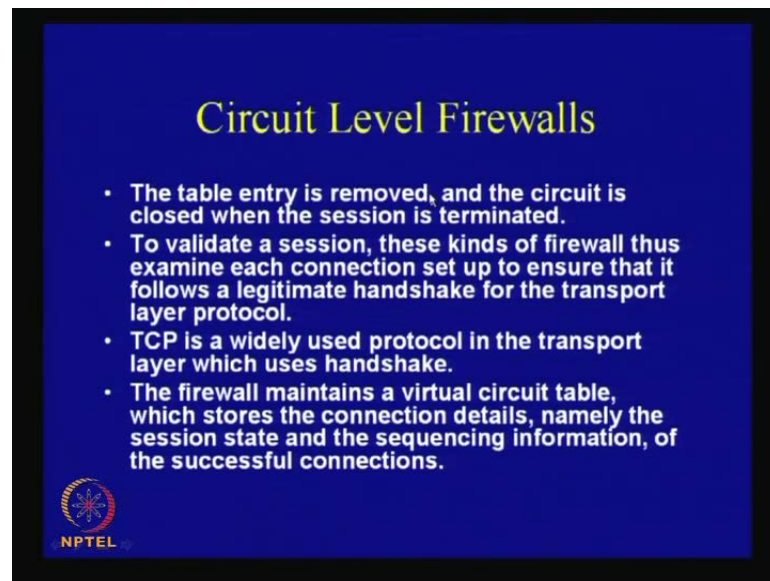
### Circuit Level Firewalls

- Circuit-level firewalls are similar in operation to packet-filtering firewalls, but they operate at the transport and session layers.
- The biggest difference between a packet-filtering firewall and a circuit-level firewall is that a circuit-level firewall validates TCP and UDP sessions before opening a connection, or circuit, through the firewall.
- When the session is established, the firewall maintains a table of valid connections and lets data pass through when session information matches an entry in the table.

  
NPTEL


So, this is an example of a cheap packet filtering tool and is often useful in the Linux based systems. So as oppose to this, we have got the other firewalls known as the circuit level firewalls, and the circuit level firewalls are similar in operation to the packet filters, but they operate at the transport and the session layers. So, the biggest difference between a packet filtering firewall and circuit level firewall is that, a circuit level firewall actually validates the TCP and UDP sessions before opening a connection or circuit through the firewall, but once this connection is established then the firewalls maintains the table of valid connection and let us data pass through when the session information matches an entry in the table. It actually does a checking before opening up the connection, but once the connection is opened up it does not do any checking of the incoming packets. Therefore, you can immediately understand that a circuit level firewall can actually be sometimes faster than a packet level of the previous kind of firewalls. Therefore, it can be faster than the packet filters.

(Refer Slide Time: 27:13)



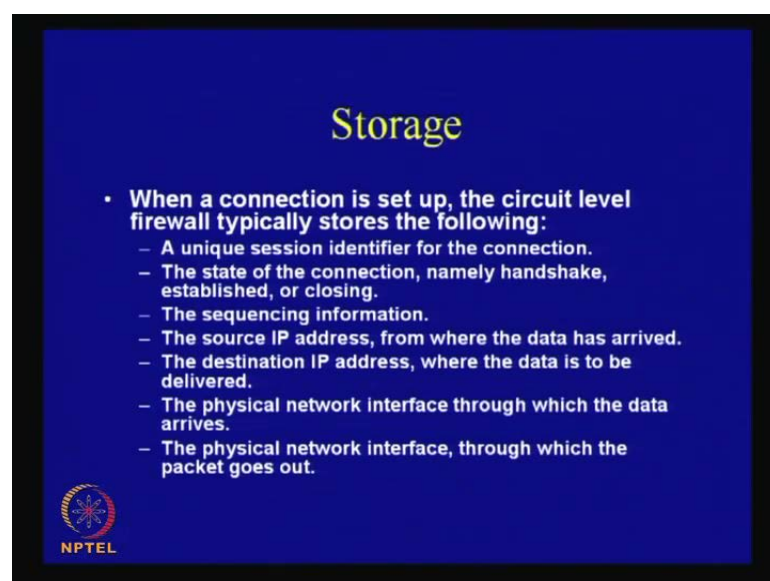
## Circuit Level Firewalls

- The table entry is removed, and the circuit is closed when the session is terminated.
- To validate a session, these kinds of firewall thus examine each connection set up to ensure that it follows a legitimate handshake for the transport layer protocol.
- TCP is a widely used protocol in the transport layer which uses handshake.
- The firewall maintains a virtual circuit table, which stores the connection details, namely the session state and the sequencing information, of the successful connections.




Now, this table entry is removed and the circuit is closed when the session is terminated to validate a session. These kinds of firewall thus examine each connection set up to ensure that it follows the legitimate handshake for the transport layer protocol. TCP is a widely used protocol and it actually uses handshake, and the firewall maintains the virtual circuit table which stores the connection details; namely the session state and the sequencing information of the successful connection.

(Refer Slide Time: 27:48)



## Storage

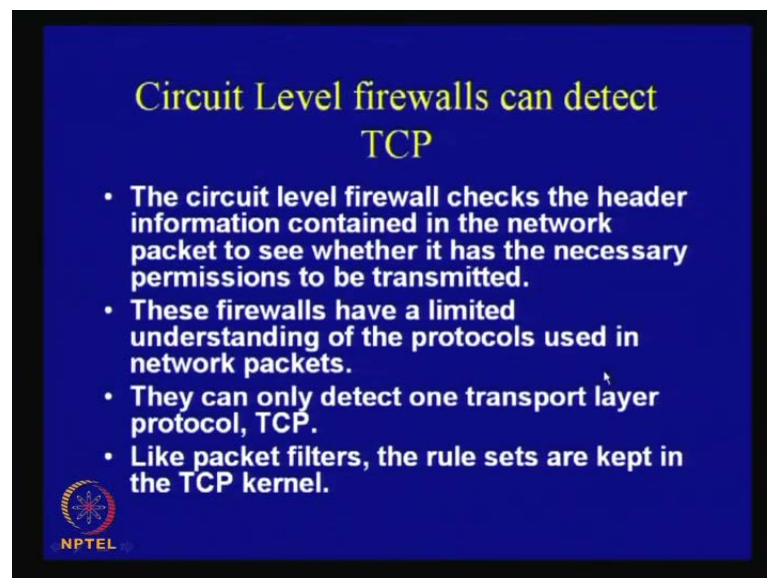
- When a connection is set up, the circuit level firewall typically stores the following:
  - A unique session identifier for the connection.
  - The state of the connection, namely handshake, established, or closing.
  - The sequencing information.
  - The source IP address, from where the data has arrived.
  - The destination IP address, where the data is to be delivered.
  - The physical network interface through which the data arrives.
  - The physical network interface, through which the packet goes out.



So, you see that it can actually maintain some amount of state information, and also some amount of sequencing information. Now, when a connection is set up the circuit level firewall typically stores the following: it will store like the unique session identifier for the connection, store the state of the connection namely handshake established or closing, store the sequencing information, store the source IP address from which the data has arrived, store the destination IP address where the data is to be delivered that is where it is going to the physical network interface through which the data arrives, the physical network interface through which the packet goes out.


So, you see that most of the storages are exactly the same as that of the packet filter; the thing which is defined is this sequencing information and the state information. Therefore, this is the significant difference of what is stored compared to the previous packet filters.

(Refer Slide Time: 28:40)



**Circuit Level firewalls can detect TCP**

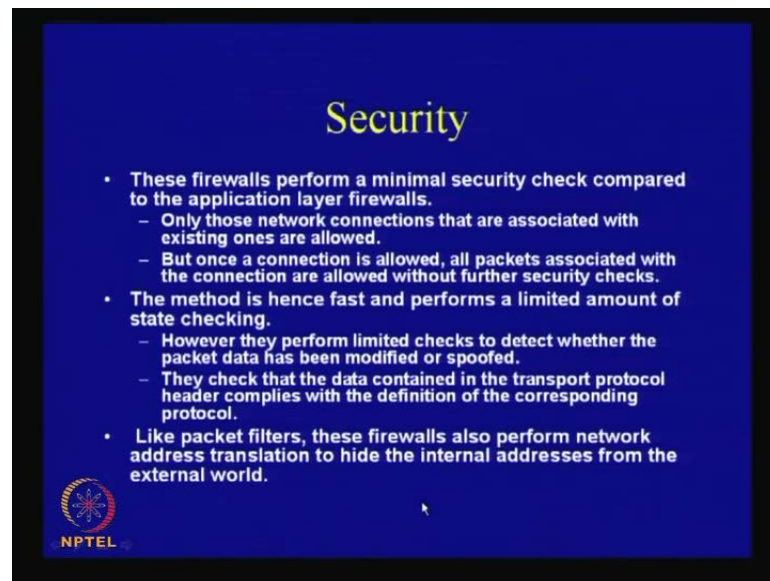
- The circuit level firewall checks the header information contained in the network packet to see whether it has the necessary permissions to be transmitted.
- These firewalls have a limited understanding of the protocols used in network packets.
- They can only detect one transport layer protocol, TCP.
- Like packet filters, the rule sets are kept in the TCP kernel.

 NPTEL

Now the circuit level firewalls can detect TCP, therefore the circuit level firewall will check the header information contained in the network packet to see whether it has the necessary permission to be transmitted. These firewalls have limited understanding of the protocols used in the networks; they would not only detect one transport layer protocol which is the TCP. Therefore, unlike the packet filters, the rules are kept in the TCP kernel. So, they are kept in the TCP kernel just like the packet filters.



(Refer Slide Time: 29:11)



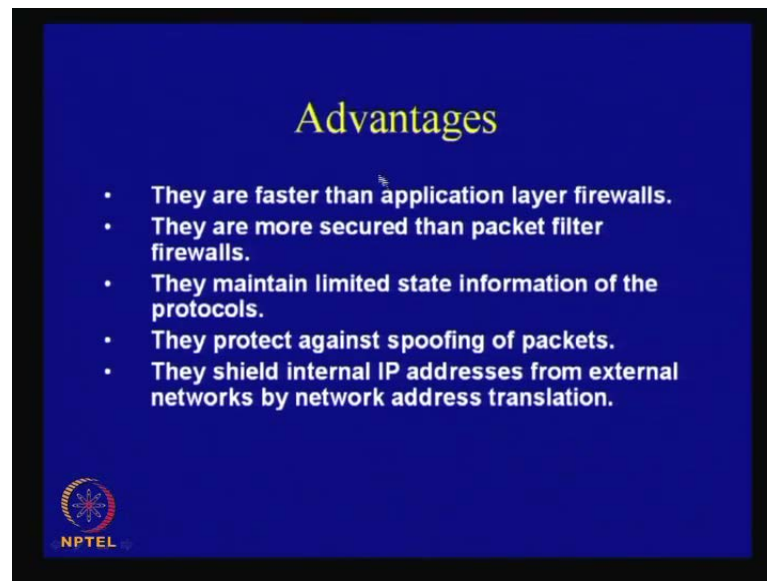
The slide is titled "Security" in a yellow serif font. It contains a list of three main bullet points, each with sub-points. The first bullet point states that these firewalls perform a minimal security check compared to application layer firewalls, with sub-points: "Only those network connections that are associated with existing ones are allowed." and "But once a connection is allowed, all packets associated with the connection are allowed without further security checks." The second bullet point states that the method is fast and performs a limited amount of state checking, with sub-points: "However they perform limited checks to detect whether the packet data has been modified or spoofed." and "They check that the data contained in the transport protocol header complies with the definition of the corresponding protocol." The third bullet point states that like packet filters, these firewalls also perform network address translation to hide internal addresses from the external world. In the bottom left corner, there is a circular logo with a globe and the text "NPTEL" below it.

- These firewalls perform a minimal security check compared to the application layer firewalls.
  - Only those network connections that are associated with existing ones are allowed.
  - But once a connection is allowed, all packets associated with the connection are allowed without further security checks.
- The method is hence fast and performs a limited amount of state checking.
  - However they perform limited checks to detect whether the packet data has been modified or spoofed.
  - They check that the data contained in the transport protocol header complies with the definition of the corresponding protocol.
- Like packet filters, these firewalls also perform network address translation to hide the internal addresses from the external world.

Now talking about security, these firewalls perform a minimal security check compared to the application layer firewalls as we will see that only those network connections that are associated with existing ones are allowed. But once a connection is allowed all packets associated with the connection are allowed without further security checks. So, once it is allowed then there is no like, once a connection has been allowed then it is included in the virtual circuit table, then the packets are not screened or not analyzed. So there is more probably security check compare to the packet filters, but it actually does less compared to the application layer firewalls, which we will discuss in the next method is hence fast and performs a limited amount of state checking. However, they perform limited checks to detect whether the packet data has been modified or spoofed.

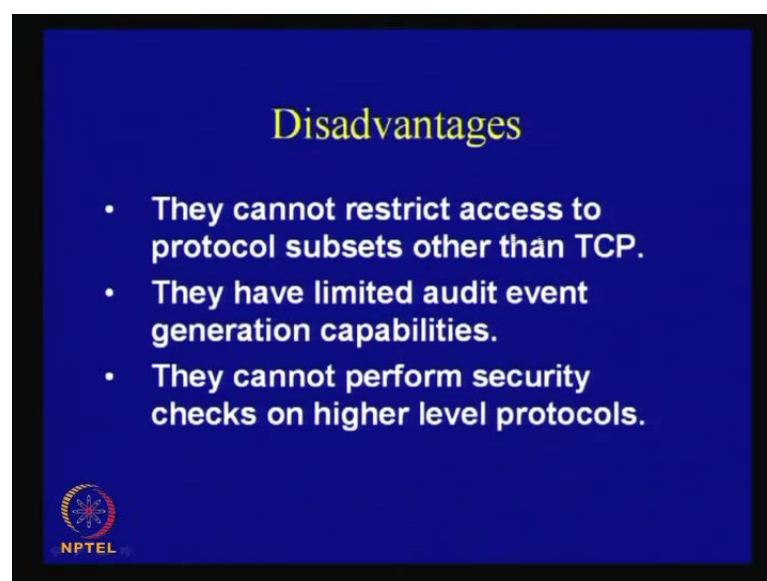
So, there is an amount of authentication involved in this kind of firewalls, they check that data contained in the transport protocol header complies with the definition of the corresponding protocol. So, like packet filters these firewalls also perform network address translation to hide the internal addresses from the external world. This feature is like similar to the packet filters, but there is a network address translation which actually hides an internal address from the external world.

(Refer Slide Time: 30:30)



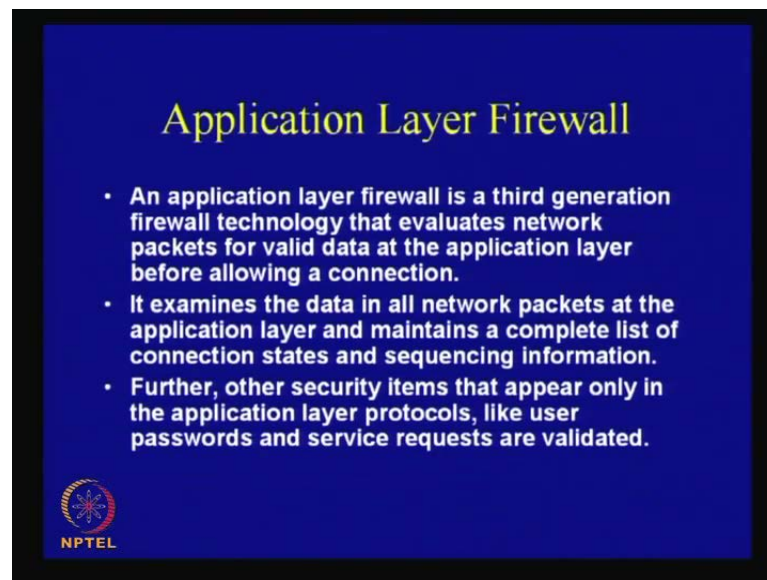
Now the advantages are, of course as you understand that they are faster than the application layer firewalls, they are more secured than the packet filter firewalls, they maintain limited state information, they maintain some amount of sequencing information, they protect against spoofing of the packets, they also shield internal IP addresses from the external networks by performing the network address translation. These are some of the advantages.

(Refer Slide Time: 30:54)



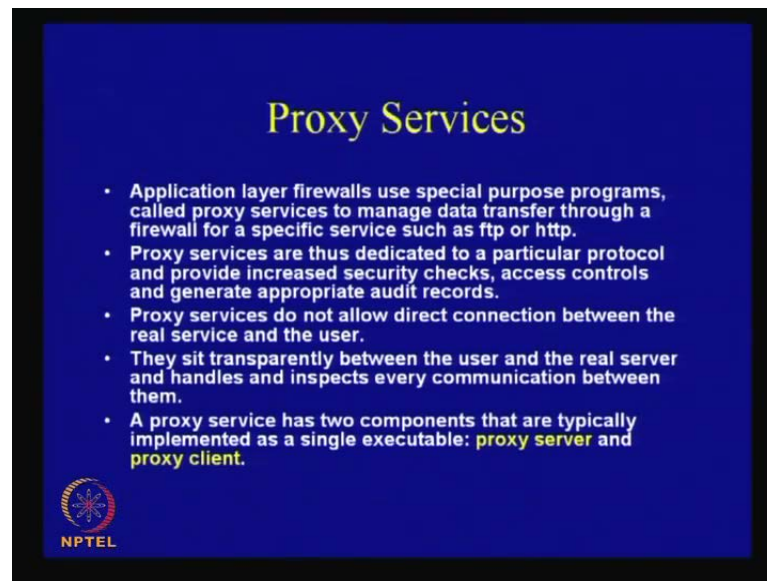
The disadvantages are it cannot restrict access to protocol subsets other than the TCP; it is only specified to TCP, they have got limited audit event generation capabilities; this is kind of limited, and they cannot perform security checks on higher level protocols; if you have got any higher level protocols then these are not meant for them.

(Refer Slide Time: 31:14)



So as oppose to this, we have got that the application layer firewalls **now the application layer firewalls** is the third generation firewall technology that evaluates the network packets for valid data at the application layer before allowing a connection. So an application layer firewall is a third generation firewall which will actually perform or it will evaluate whether a particular data is valid or other is allowed or not, and it actually examines data in all network packets at the application layer and maintains a complete list of connection states and sequencing information. Here, the documentation or the auditing is much more complete as oppose to the previous firewalls. It actually maintains a complete list of the states of the connections and the corresponding sequence information. Now, further other security items that appear only in the application layer protocols like user passwords and service requests are also validated. So here, we see that these kinds of firewalls are actually meant for the high level protocols, they have got more state information and they maintain better sequencing information of the corresponding protocols.

(Refer Slide Time: 32:25)



The slide has a dark blue background with yellow text. The title 'Proxy Services' is centered at the top. Below it is a bulleted list of five points. The last point includes the terms 'proxy server' and 'proxy client' in yellow. In the bottom left corner, there is a circular logo with a red and blue design and the text 'NPTEL' below it.

## Proxy Services

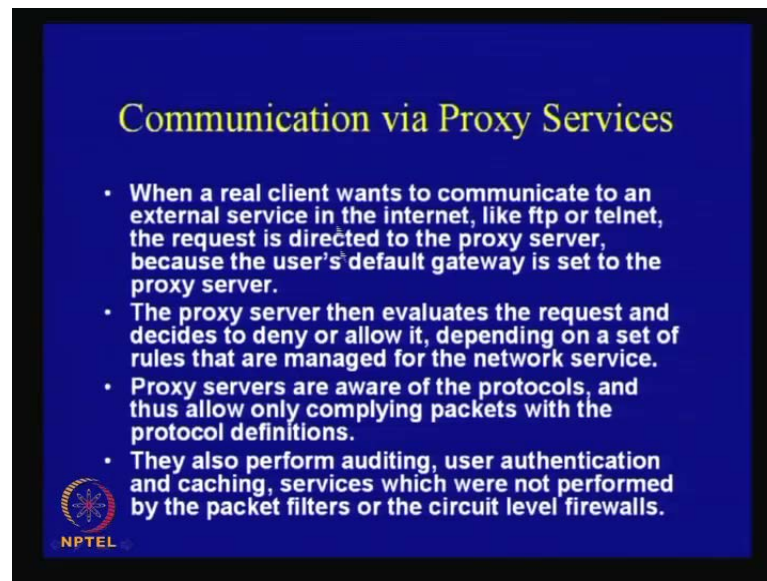
- Application layer firewalls use special purpose programs, called proxy services to manage data transfer through a firewall for a specific service such as ftp or http.
- Proxy services are thus dedicated to a particular protocol and provide increased security checks, access controls and generate appropriate audit records.
- Proxy services do not allow direct connection between the real service and the user.
- They sit transparently between the user and the real server and handles and inspects every communication between them.
- A proxy service has two components that are typically implemented as a single executable: proxy server and proxy client.

NPTEL

Now, the application layer firewalls use special purpose programs which are actually called proxy services to maintain data transfer through a firewall for a specific service such as FTP or HTTP. Therefore, special purpose programs are used inherently in these kinds of firewalls. Proxy services are dedicated to a particular protocol and provide increased security checks, access controls, and generate appropriate audit records. Now these proxy services of course as you understand that, if they perform so much amount of auditing, and it performs so much amount of security check, it come with the accompanying disadvantage of making the system must slow.


Therefore, these kinds of firewalls that is the application layer firewalls are nearly slow in nature; extremely slow. So proxy services actually do not allow the direct connection between the real service and the user. They sit between the user and the real server and handles and inspects each and every communication between them, but of course it ensures that it is a transparent it sits transparently that is the user and the real server does not understand that a proxy server; a program is actually monitoring them.

(Refer Slide Time: 33:51)



**Communication via Proxy Services**

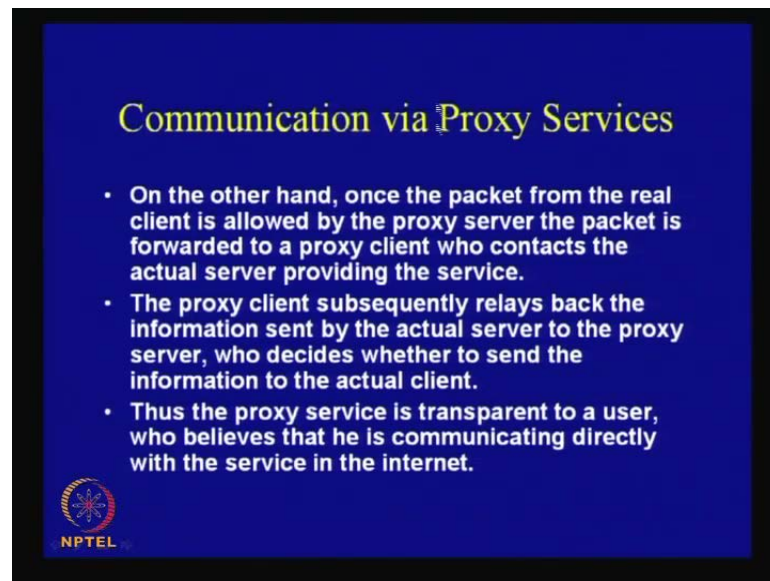
- When a real client wants to communicate to an external service in the internet, like ftp or telnet, the request is directed to the proxy server, because the user's default gateway is set to the proxy server.
- The proxy server then evaluates the request and decides to deny or allow it, depending on a set of rules that are managed for the network service.
- Proxy servers are aware of the protocols, and thus allow only complying packets with the protocol definitions.
- They also perform auditing, user authentication and caching, services which were not performed by the packet filters or the circuit level firewalls.

 NPTEL

Now, a proxy service has got typically two components and it is often implemented as a single executable, one is the server; the proxy server, and the client; the proxy client. The proxy server and the proxy client has got the functions like when a real client wants to communicate to an external service in the network like FTP or telnet, the request is directed to the proxy server because the users default gateway is set to the proxy server. Therefore, when a real clients wants to communicate or others, you can think like it wants, you can imagine like the (( )) network there is a user which wants to access an external service in the internet, then the request is first directed to the proxy server.


So, a proxy server actually is sitting near because the users default gateways is set to the proxy server, the proxy server gets the information and then evaluates the request and decides to deny or allow depending upon its rules which was actually maintained by the network. The proxy servers are aware of the protocols and therefore, allow only complying packets within the protocol definitions.

(Refer Slide Time: 34:59)



**Communication via Proxy Services**

- On the other hand, once the packet from the real client is allowed by the proxy server the packet is forwarded to a proxy client who contacts the actual server providing the service.
- The proxy client subsequently relays back the information sent by the actual server to the proxy server, who decides whether to send the information to the actual client.
- Thus the proxy service is transparent to a user, who believes that he is communicating directly with the service in the internet.

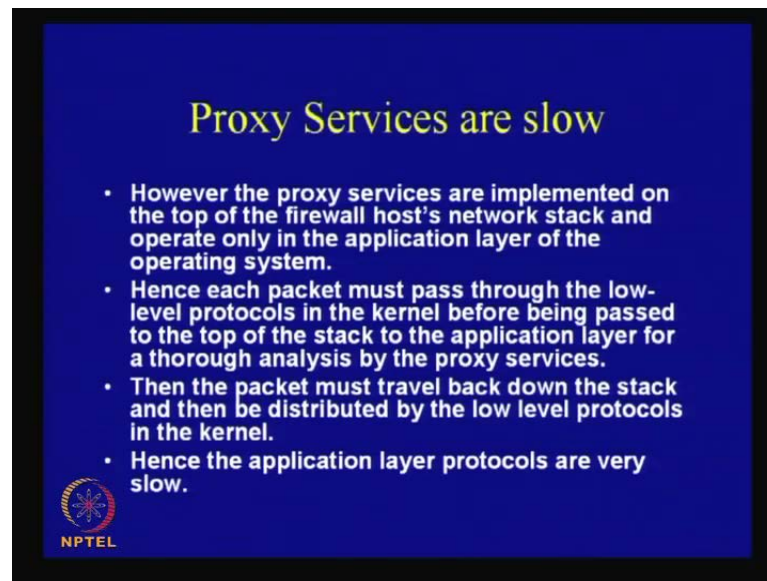
 NPTEL

They also perform auditing user authentication and caching services which were not performed by the previous firewalls. So on the other hand, once a packet from the real client is allowed by the proxy server, the packet is forwarded to the proxy client **So the proxy client receives it after this** who contacts the actual service providing server. That is the server which is sitting in the external network, and the proxy client subsequently relays back the information sent by the actual server to the proxy server who decides whether to send information to the actual client.

So the proxy server is thus, you see as it is transparent to the user who believes that he is he is actually communicating directly with the service in the internet. But actually it is communicating via the proxy server and the proxy client which together actually makes the proxy service.




(Refer Slide Time: 35:45)



### Proxy Services are slow

- However the proxy services are implemented on the top of the firewall host's network stack and operate only in the application layer of the operating system.
- Hence each packet must pass through the low-level protocols in the kernel before being passed to the top of the stack to the application layer for a thorough analysis by the proxy services.
- Then the packet must travel back down the stack and then be distributed by the low level protocols in the kernel.
- Hence the application layer protocols are very slow.

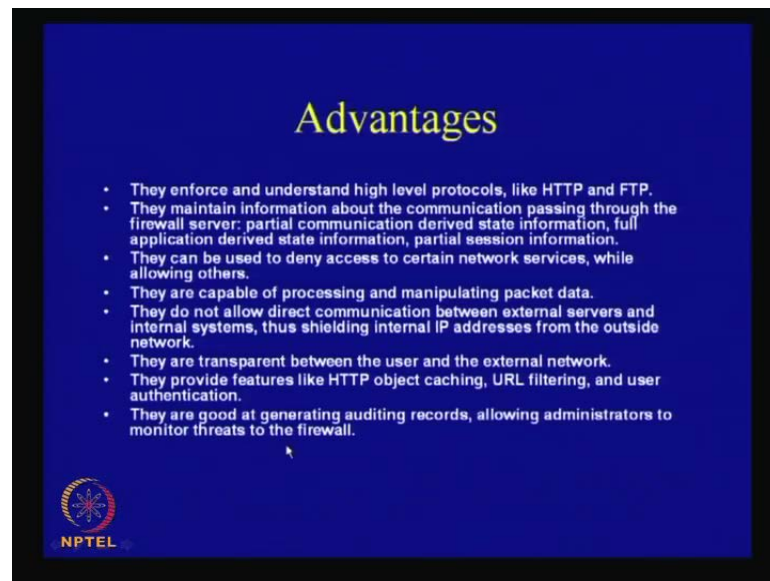


NPTEL

Therefore, proxy services as you understand are slow, because it makes the entire network slow. However, the proxy services are implemented on top of the firewalls hosts network stack and operate only in the application layer of the operating system. Hence each packet must pass through the low level protocols in the kernel before being passed to the top of the stack to the application layer for a thorough analysis by the proxy services. So the idea is that, the proxy servers or proxy services are implemented using the network stacks, therefore the idea is that whenever a packet comes it has to move through the networks stack and come to the server or the service. And we analyzed that again when it is communicated back it passes to those stacks and go back.

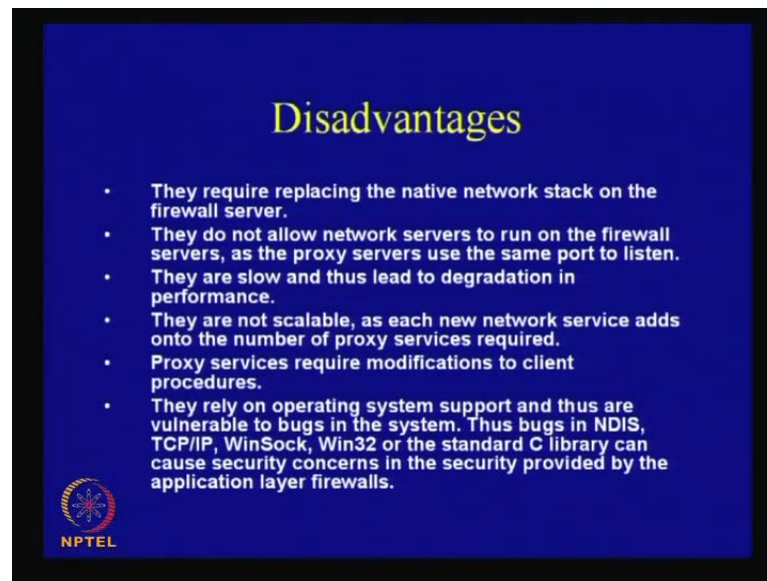
Therefore, the idea is that the entire process becomes extremely slow, and if you want for example speeding in your network then you have to actually use it carefully like you have to use it. So I mean, if you want a kind of, I mean your time is also a constant like if you want it has to performed online or it has to be performed in real time, then you actually have to use these kind of firewalls in a more sensible manner. So, that is one challenging part of this kind of firewalls.

(Refer Slide Time: 37:10)




So the advantages are that, they enforce and understand high level protocols like HTTP and FTP, they maintain information about the communications passing through the firewall servers; it has got lot of state information. They can be used to deny accesses to certain network services while allowing others, so they are also capable of processing and manipulating the packer data. They do not allow direct communication between the external servers and internal system; therefore it shields the internal IP addresses from the outside network. They are transparent between the user and the external network, and provide features like HTTP object caching URL filtering and user authentication. They are good at generating auditing records which actually can allow or help the administrators to monitor threats to the firewalls.

(Refer Slide Time: 37:56)



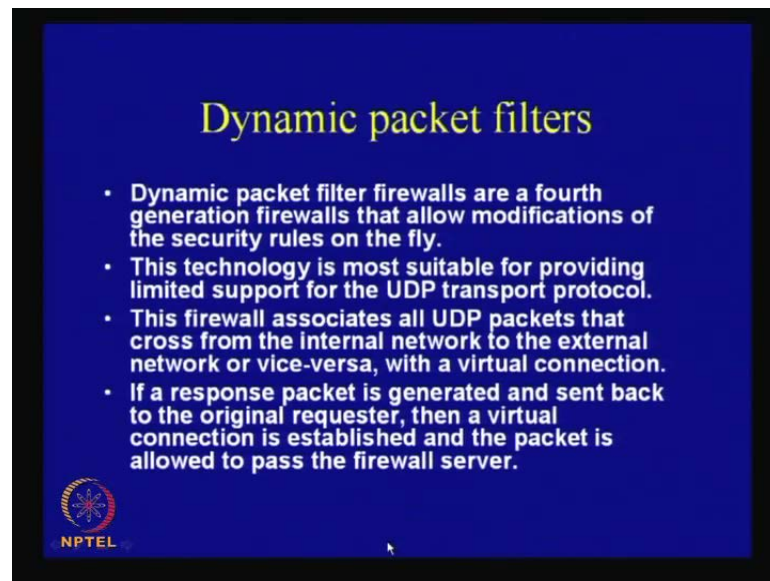
## Disadvantages

- They require replacing the native network stack on the firewall server.
- They do not allow network servers to run on the firewall servers, as the proxy servers use the same port to listen.
- They are slow and thus lead to degradation in performance.
- They are not scalable, as each new network service adds onto the number of proxy services required.
- Proxy services require modifications to client procedures.
- They rely on operating system support and thus are vulnerable to bugs in the system. Thus bugs in NDIS, TCP/IP, WinSock, Win32 or the standard C library can cause security concerns in the security provided by the application layer firewalls.




Now it has got some disadvantage as well, as we know one of them is the speed. They require replacing the native network stack on the firewall server, so they need these kinds of modifications. They do not allow network servers to run on the firewall servers as the proxy servers use the same port to listen, so they are slow and thus lead to degradation in performance. They are not scalable as each new network service adds onto the number of proxy services which are required. Proxy services require modifications to client procedures; they rely on operating system support and thus are vulnerable to bugs in the system. Therefore, if there are bugs in the systems like as we have seen in the previous cases about there could be bugs in the standard C library, then it cause security concerns in the security provided by the application layer firewalls. So, they actually rely on operating systems as if they are bugs in the operating system then this kind of firewalls can be vulnerable to threats.

(Refer Slide Time: 39:05)



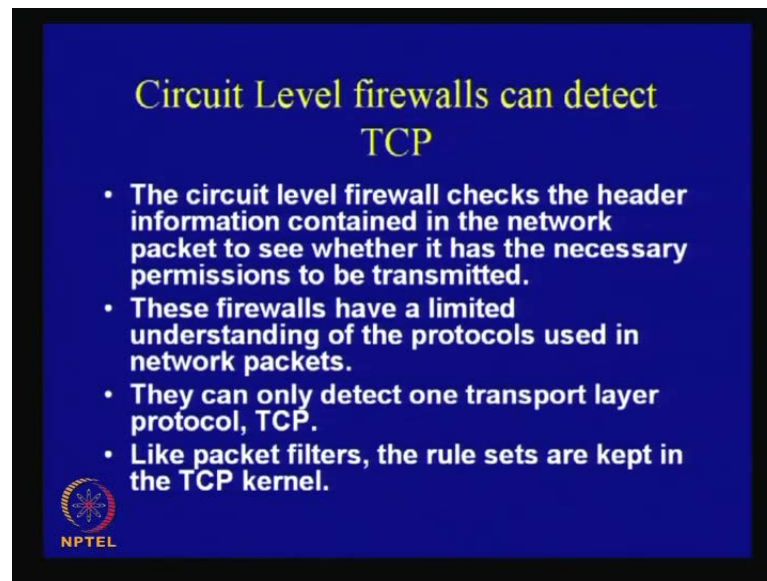
**Dynamic packet filters**

- Dynamic packet filter firewalls are a fourth generation firewalls that allow modifications of the security rules on the fly.
- This technology is most suitable for providing limited support for the UDP transport protocol.
- This firewall associates all UDP packets that cross from the internal network to the external network or vice-versa, with a virtual connection.
- If a response packet is generated and sent back to the original requester, then a virtual connection is established and the packet is allowed to pass the firewall server.

 NPTEL


Now, we have got a fourth generation firewall which is actually known as the dynamic packet filters. So, these dynamic packet filters are actually the fourth generation firewalls that allow modifications of the security rules on the fly, so it is a kind, as a name suggest it is dynamic. Therefore, the security rules are not static, and they are modified on the fly. This technology is most suitable for providing limited support for the UDP transport protocol, so as we have seen that it actually extends to the UDP transport protocols like which was not supported by the application layer firewalls. So this firewall associates all the UDP packets that cross from the internal network to the external networks or vice versa with a virtual connection. If a response packet is generated and sent back to the original requester, then a virtual connection is established and the packet is allowed to pass the firewall server.

(Refer Slide Time: 40:27)



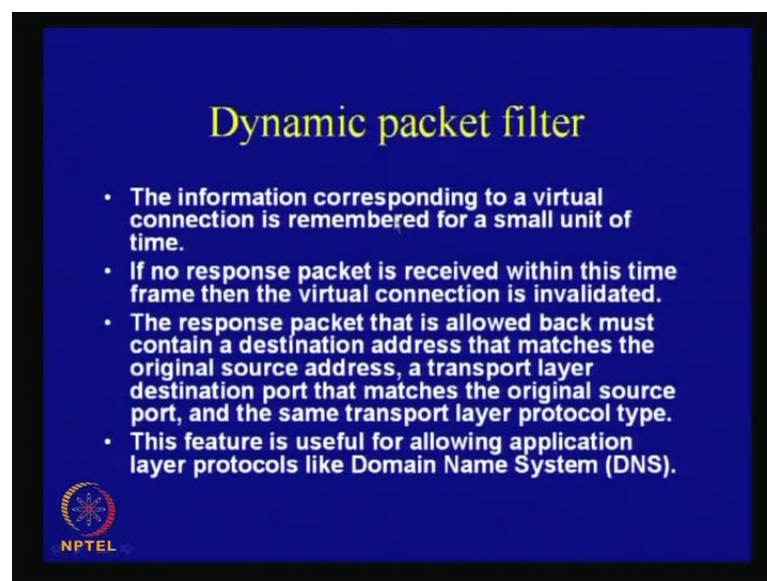
**Circuit Level firewalls can detect TCP**

- The circuit level firewall checks the header information contained in the network packet to see whether it has the necessary permissions to be transmitted.
- These firewalls have a limited understanding of the protocols used in network packets.
- They can only detect one transport layer protocol, TCP.
- Like packet filters, the rule sets are kept in the TCP kernel.

 NPTEL


Therefore, we see that one of the advantages is that this supports the UDP packets, and it maintains a dynamic set of rules which allows or denies an incoming or outgoing packet. This is an oppose to the previous things as we have seen here like, when we consider the circuit level protocols then they only were used to detect one transport layer protocol which is the TCP.

(Refer Slide Time: 40:52)



**Dynamic packet filter**

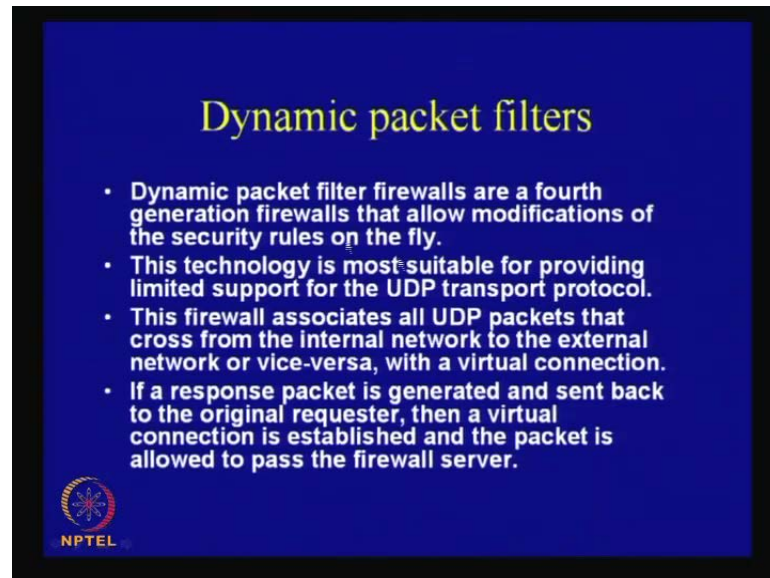
- The information corresponding to a virtual connection is remembered for a small unit of time.
- If no response packet is received within this time frame then the virtual connection is invalidated.
- The response packet that is allowed back must contain a destination address that matches the original source address, a transport layer destination port that matches the original source port, and the same transport layer protocol type.
- This feature is useful for allowing application layer protocols like Domain Name System (DNS).

 NPTEL

Therefore, they were not applicable for the UDP, but on the other hand, this is actually helping us to extend the security checks to the UDP networks and UDP protocols as


well. So now, the information corresponding to a virtual connection is remembered for a small unit of time.

(Refer Slide Time: 41:03)



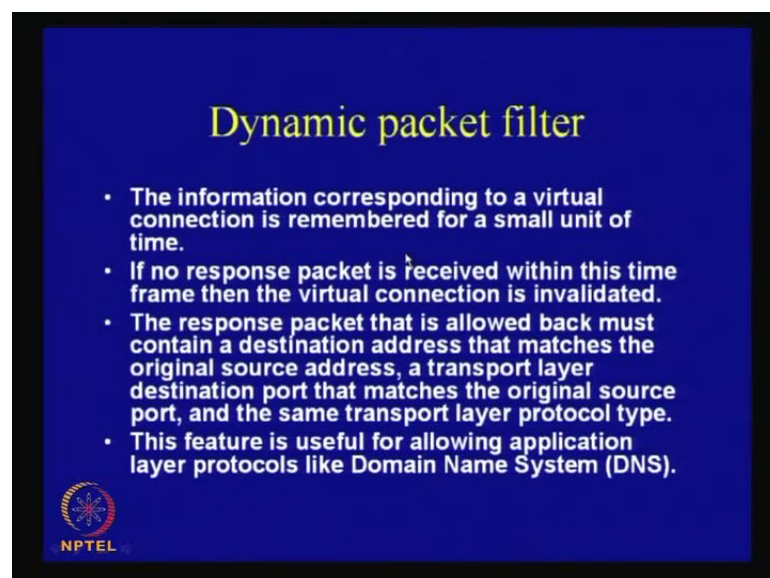
### Dynamic packet filters

- Dynamic packet filter firewalls are a fourth generation firewalls that allow modifications of the security rules on the fly.
- This technology is most suitable for providing limited support for the UDP transport protocol.
- This firewall associates all UDP packets that cross from the internal network to the external network or vice-versa, with a virtual connection.
- If a response packet is generated and sent back to the original requester, then a virtual connection is established and the packet is allowed to pass the firewall server.




Therefore, if there is no response during this time then within the time frame the virtual connection is invalidated. In these kinds of dynamic packet or this kind of filters, **in dynamic packet filters** if the response packet is generated and sent back to the original requester then a virtual connection is established and the packets are allowed to pass the firewall server.

(Refer Slide Time: 41:29)



### Dynamic packet filter

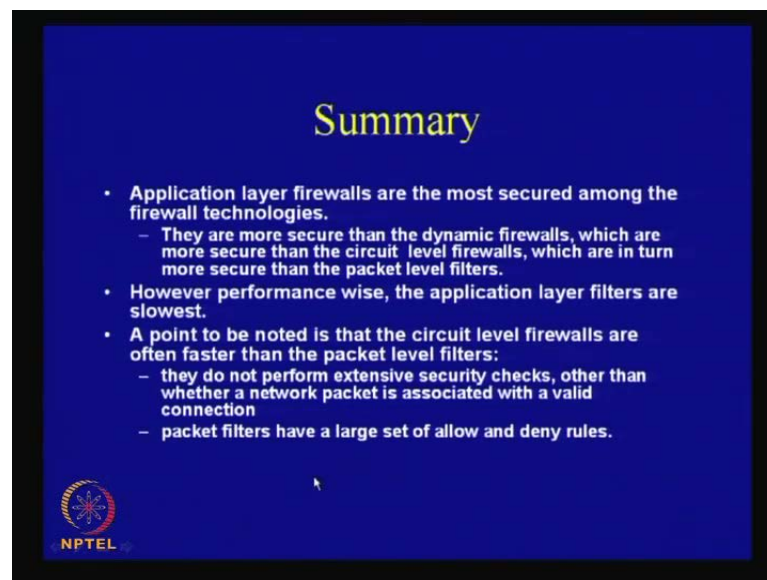
- The information corresponding to a virtual connection is remembered for a small unit of time.
- If no response packet is received within this time frame then the virtual connection is invalidated.
- The response packet that is allowed back must contain a destination address that matches the original source address, a transport layer destination port that matches the original source port, and the same transport layer protocol type.
- This feature is useful for allowing application layer protocols like Domain Name System (DNS).





But if the response is not received within a particular time quanta, then this virtual connection is stopped and the packets are not allowed to pass. So, if no response received within this time frame then the virtual connection is actually invalidated. Now, the response packet that is allowed back must contain a destination address that matches the original source addresses or transport layer destination port. Therefore, it has to have a destination address that matches the original source address, and a transport layer destination port that matches the original source port, and the same transport layer protocol type that is the exact transport layer protocol type which is being used.

(Refer Slide Time: 42:12)



**Summary**

- Application layer firewalls are the most secured among the firewall technologies.
  - They are more secure than the dynamic firewalls, which are more secure than the circuit level firewalls, which are in turn more secure than the packet level filters.
- However performance wise, the application layer filters are slowest.
- A point to be noted is that the circuit level firewalls are often faster than the packet level filters:
  - they do not perform extensive security checks, other than whether a network packet is associated with a valid connection
  - packet filters have a large set of allow and deny rules.

NPTEL

Now, this feature is useful for allowing applications layer protocols like the DNS or the domain name systems. So the summary of what we have seen here is the application layer firewalls. You would be interested to understand about the comparisons among the existing firewall technologies. Therefore, the application layer firewalls are the most secured among the existing firewall technologies, and they are more secure than the dynamic firewalls which are again more secure than the circuit level firewalls which are in turn more secure than the packet level filters.

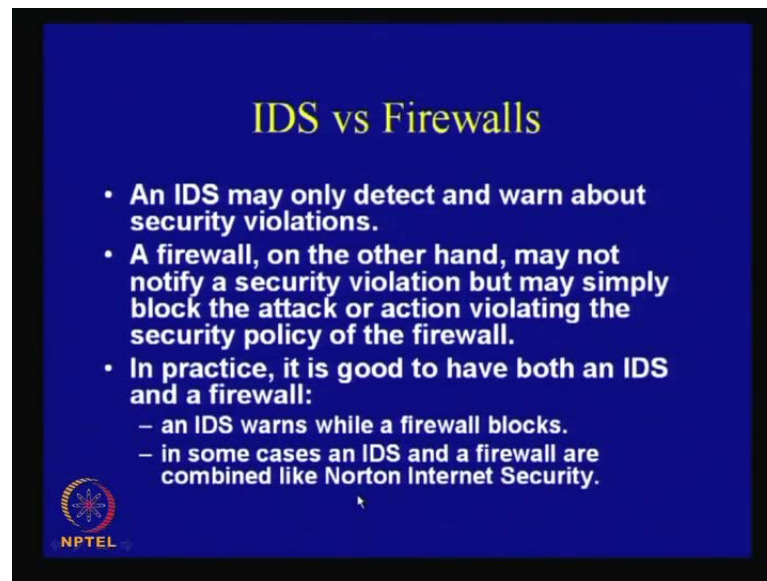
Therefore, you consider that the most secured among all the firewalls is the application layer firewalls, and the least secure is the packet level firewalls. However, performance wise the application layer firewalls or the filters or firewalls are actually slowest. They are the slowest because as we all know that because of the proxy services the proxy

services are inherently slow. They essentially inspect each and every packet which is being communicate by the user with the external service and therefore, they are essentially slow in nature, and also they have to perform or they have to essentially each and every packet has to pass to the entire network stack. So that actually makes the entire process extremely slow, and there is also large number of auditing involved. Therefore, application layer firewalls actually performs lot of auditing, everything actually comes around with an accompanying time involved, and therefore it is inherently slow in nature.

On the other hand, the packet layer filters are actually quite fast because they do some minimal check. Point to be noted is actually the circuit level firewalls are often faster than the packet level filters, this is a point which is to be stressed. So, as we have seen that although the circuit level firewalls has got more security than the packet level firewalls, but they are actually sometimes more faster than the packet level filters. It is because they often do not perform the extensive security checks other than whether a network packet is associated with a valid connection. So as we have seen that, once a network packet is associated with a valid connection they do not perform extensive security checks, therefore the packets are subsequently passed without checking.


So packet filters have got on the other hand, a large set of allow and deny rules, therefore there is a large in the large network actually there will be a huge number of allow and deny rules which can actually make your packet filters slower than the circuit level firewalls.

(Refer Slide Time: 44:38)



**IDS vs Firewalls**

- An IDS may only detect and warn about security violations.
- A firewall, on the other hand, may not notify a security violation but may simply block the attack or action violating the security policy of the firewall.
- In practice, it is good to have both an IDS and a firewall:
  - an IDS warns while a firewall blocks.
  - in some cases an IDS and a firewall are combined like Norton Internet Security.

 NPTEL

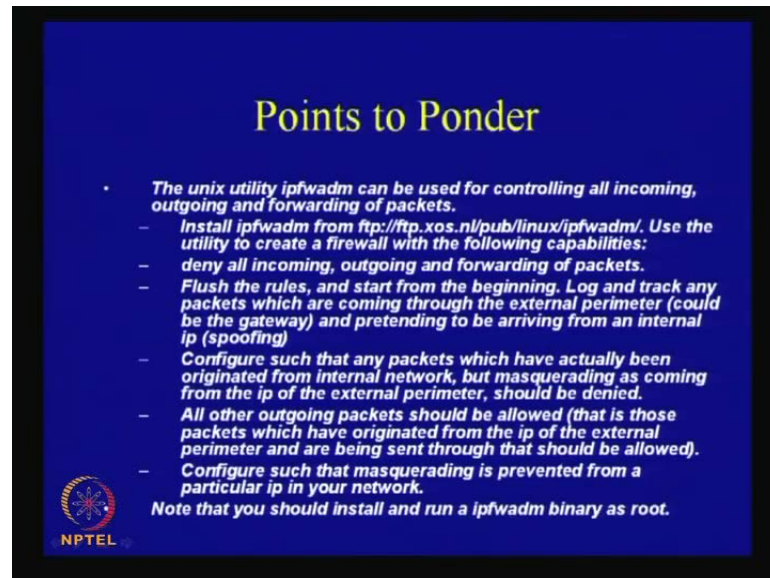
Now the other important or the other accompanying question which can come up is, like is an IDS a substitute for a firewall or a firewall be a substitute for an IDS. So the message is that, I mean they are not actually computing technologies. Therefore, it is a kind of accompanying or complimenting technology, so an IDS may only detect and warn about security violations. The idea of an IDS is kind of, to do the (( )) it will observe the network and see that whether they are any existing security violations.

On the other hand, a firewall will actually not necessarily notify about a security violations. Therefore, as we have said that IDS although it prevents, the main job of an IDS is actually to monitor the network and to see whether there is any security violations in actually document and perform auditing that is, it actually helps the system administrator to understand the security threats. The job of a firewall is on the other hand not to notify the security violations, that is not the prime job of a firewall. It may be is to simply block the attack or take some actions or block the attack or block the action which actually violates the security policy of the firewall. So, it could like without even notifying the network administrator it can simply block the particular attack and can prevent threats to the network.

So, in practice it is actually good to combine both an IDS and firewall. We can say that an IDS warns while a firewall blocks, therefore the main objective of an IDS is to warn while the main objective of a firewall is actually to block. no but actually then new

generation it is generally combine like We do not generally draw a line between IDS and firewall, so it is kind of a combined technology nowadays and for example, we can find in the Norton internet security where an IDS and firewall is being combined.


(Refer Slide Time: 46:39)



### Points to Ponder

- *The unix utility ipfwadm can be used for controlling all incoming, outgoing, and forwarding of packets.*
  - *Install ipfwadm from <ftp://ftp.xos.nl/pub/linux/ipfwadm/>. Use the utility to create a firewall with the following capabilities:*
    - *deny all incoming, outgoing and forwarding of packets.*
    - *Flush the rules, and start from the beginning. Log and track any packets which are coming through the external perimeter (could be the gateway) and pretending to be arriving from an internal ip (spoofing)*
    - *Configure such that any packets which have actually been originated from internal network, but masquerading as coming from the ip of the external perimeter, should be denied.*
    - *All other outgoing packets should be allowed (that is those packets which have originated from the ip of the external perimeter and are being sent through that should be allowed).*
    - *Configure such that masquerading is prevented from a particular ip in your network.*

*Note that you should install and run a ipfwadm binary as root.*

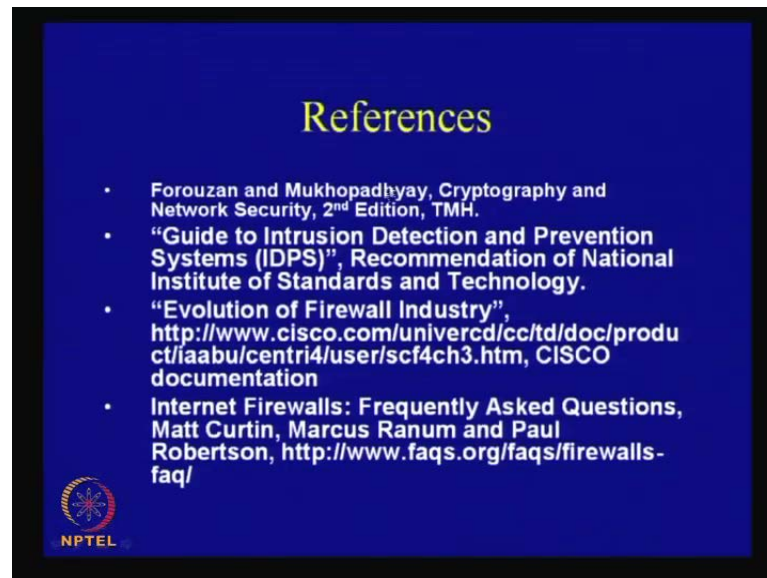
 NPTEL

So, here is a small exercise which you can try is the UNIX utility. As we have said, ipfwadm can be used for controlling all incoming, outgoing and forwarding of packets. So we can do this, we can install this packet from this particular URL which is provided, and we can use the utility to create a firewall with the following capabilities like, we can try to deny all the incoming, outgoing and forwarding of packets. We can flush the rules and start from the beginning, so log and track any packets which are coming through the external perimeter it could be the gateway and pretending to be arriving from an internal IP that is case of spoofing. Therefore, this can be tackled, we can also configure using this ipfwadm tool, such that any packets which have actually been originated from internal network, but masquerading as coming from the IP of the external perimeter, should be denied.

So, these are some of the important steps which can be taken by these kinds of packet filters. All other outgoing packets should be allowed that is those packets which have originated from the IP of the external perimeter are being sent through should be allowed. Now, we can also configure such that masquerading is prevented from a particular IP in your network. So these are some policies which can be enforced in our

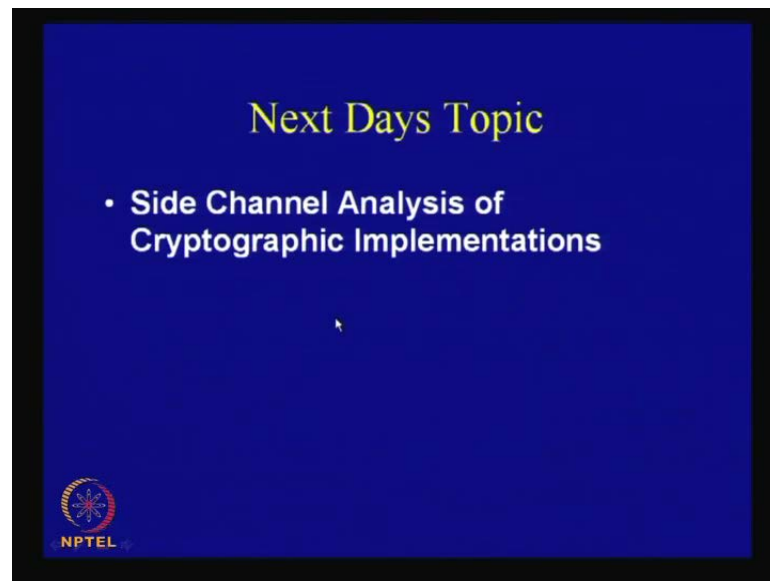
network, and we can actually try to see that whether we can use the ipfwadm tool and we can enforce these policies. So, note that you should install and run this ipfwadm tool binary as a root to your system. Therefore, this can be a simple exercise which we can practice to understand the basics of packet filtering.

(Refer Slide Time: 48:32)



Now, some of the references that we have followed for our text are these books. So this book is like guide to intrusion detection and prevention systems IDPS. You can also refer to evolution of firewall industry, the corresponding URL is given; it is a CISCO documentation. The other reference is internet firewalls and some frequently asked questions, and it is a very interesting read. Therefore, all of you are encouraged to read this; it is a very nice read.

(Refer Slide Time: 49:02)



And next day, we shall take up the topic of side channel analysis of cryptographic implementations. So, this will be the concluding topic, we have till now talked about some of the important parts of network security, and we shall actually conclude our discussions on class with an important topic which is called as side channel analysis without which the discussion of cryptography and security will not be complete.