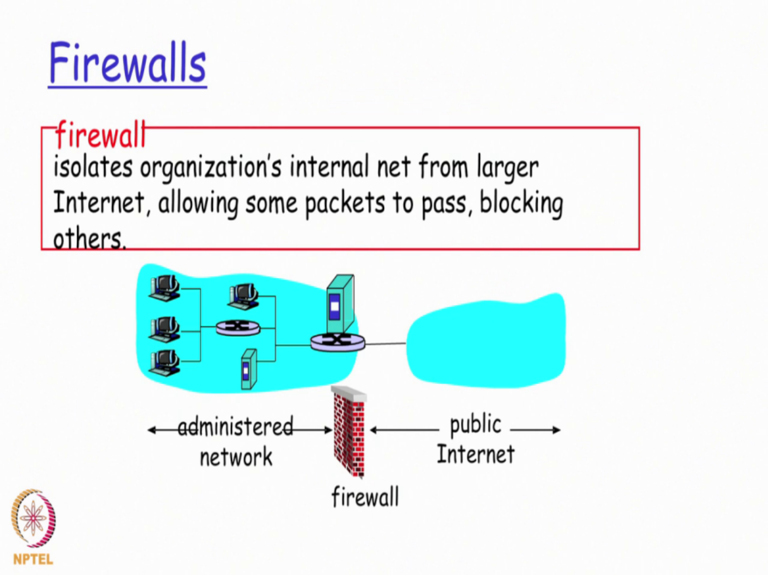
Information Security 3
Sri M J Shankar Raman,
Consultant Department of Computer Science and Engineering,
Indian Institute of Technology Madras
Module 55
Security in Practice

In this module onwards we will actually try to see a set of products or tools that are typically deployed on the network security point of view and why they are very critically required for any kind of a network topology in an organization.

(Refer Slide Time: 00:30)



Firewalls

firewall
isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.

So one of the first kinds of devices from the network security point of view that we will very commonly come across is something called as a firewall, so what exactly is a firewall and what is it actually trying to do.

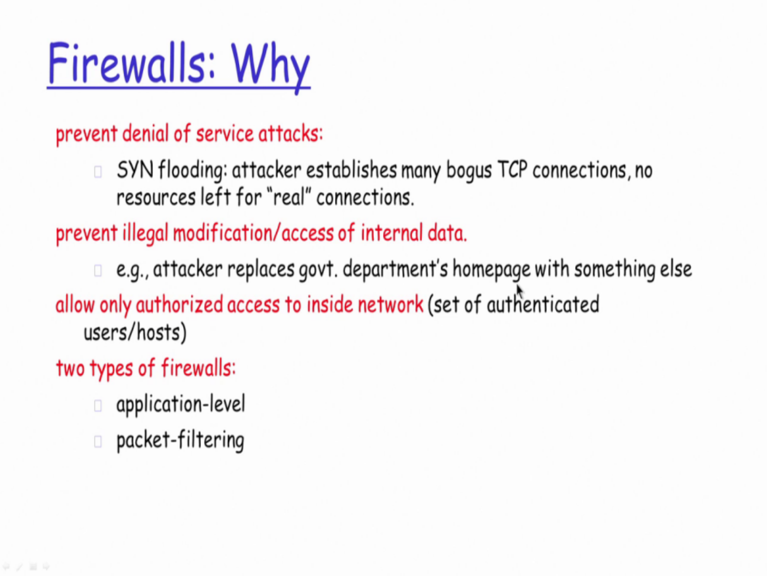
So firewall is a device that typically tries to isolate the organizations internal and the external network, so the external network here would be typically the the internet to which the organization would want to be connected to for doing its business activities right, so through this firewall the administrator would typically want to control of what packets basically pass through or allowed to be pass through and what kind of packet should be typically block.

So if you see here if I basically have this part of my network connected internally as part of my own organization network topology and I have a public internet through my isp to which I am connected to right, so I might have a router device here in which my public internet will be terminating and I also will have my intranet getting terminated on this router device right, so I will typically have a firewall device just before this router device or as part of this router device itself.

Depending on the size of my network, now this firewall device is going to act as the sort of an interface or a bridge between my administered network that is basically my local intranet and my public internet and I would have configurations done on this firewall device basically mentioning what kind of packets are to be allowed to basically get out of my intranet into the internet as well as what kind of packets are allowed to come from the public internet

Into my intranet to the extent of specifying what servers are missions inside my network alone or capable of receiving those packets right, so all these things are typically done in the firewall and that is why the firewall is something which is a very very critical device which has to be mandatorily setup in any kind of a organizational network.

(Refer Slide Time: 02:41)



Firewalls: Why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections.

prevent illegal modification/access of internal data.

- e.g., attacker replaces govt. department's homepage with something else

allow only authorized access to inside network (set of authenticated users/hosts)

two types of firewalls:

- application-level
- packet-filtering

So one of the common things that the firewall is expected to do as a very set of critical activities is first it is expected to prevent.

Denial of service attacks, now what exactly is a denial of service, so denial of service is shortly refer to as dos right, so we would have actually heard in quite of few situations in our professional carrier where we might have read about and even experienced these kinds of dos attacks, no what exactly is a denial of service attack is that if external hacker wants to basically bring down a part of my network or a very critical server in my network.

The person will basically try to see how the the resources on that particular server can actually be completely made use of thereby the resources not becoming available for legitimate connections that I might be getting on that server from outside my network right, so the attacker or the hacker will basically try to ensure that if for example memory is a critical resource on that particular system, what all activities can you do to completely make use of the memory in a very bogus manner.

To such an extent that if there is a legal legitimate connection that is actually coming in that same server for that particular connection the server might not have the enough memory to be allocated right, so how is this actually possible so one type of a denial of service attack is what is called as SYN flooding, now if we learn about something called as a TCP protocol there is there is a a three way handshake that the TCP protocol that is required for any kind of data transfer to take place.

Over a reliable TCP connection right, now this kind of three way handshake is required to be completed before I could really start transferring the data, now an attacker will typically what he will actually try to do here is that instead of completing the entire three way handshake right, so from the client to the server the acknowledgement from the server to the client and the final acknowledgement from the client to the server so that is the reason.

Why we call it as a three way handshake so instead of really completing all the three phases of this handshake the attacker will basically keep the connection in a sort of an incomplete state for a very long period of time because of which whatever memory resources is actually been allocated by the server side, the server will not be in a position to make use of that for using those resources for legitimate connections that is actually coming in from the clients which wants to complete.

The three way handshake completely right, so thereby the attacker in this particular case will be bombarding this particular server with a heavy amount of SYN packets without really completing the entire connection right, so the memory buffers that was actually available for the the server to handle all the incoming connections will be actually made use of for servicing these kind of bogus incomplete connections that this attacker is inducing into that particular server.

Because of which a legitimate client will not be able to successfully get connected under this server and get possibility of using this server for doing any kind of service that it is expecting from the server right, so firewalls today are expected to detect all these kind of different possible dos attacks and prevent them with a different configurations that are typically done on the firewall device right, now the second thing that the firewall device is expected to do.

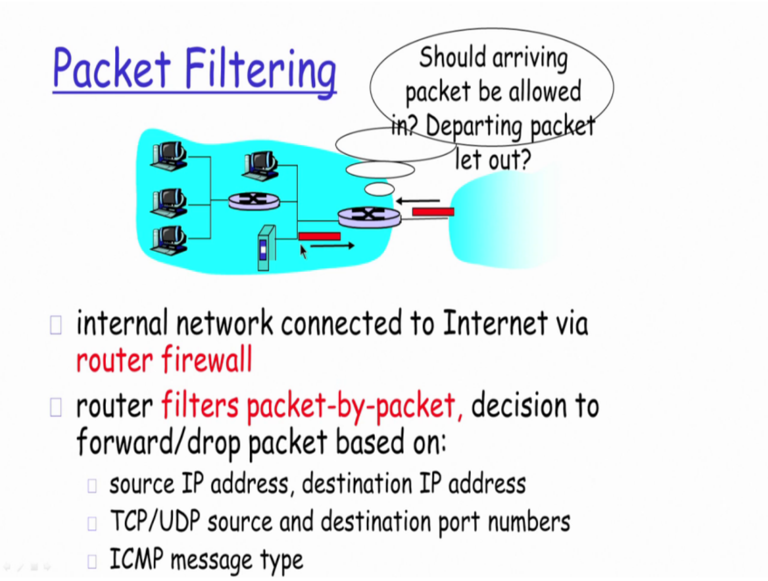
Is prevent illegal modifications or access of internal data so I do not obviously want if my for example I am running a business organization I don’t want my competitor to get access to any kind of my customer data because of which my business is at a huge risk right, or for for for example if my internal network is basically a government departments network, I do not want a unauthorized person coming from the outside internet to access all the confidential data.

That the government might me actually having as part of its intranet right, so irrespective of whatever is a usage, the firewall is expected to provide the a protection mechanism by which I will be able to set policies on what all kinds of servers or data that an external person can physically access from the public internet right, so I should be able to make these kind of configuration changes set up in the firewall to either enable or disable selectively of who can actually get control.

Of the data that is actually available as part of my intranet, third allows only authorized access to inside network so essentially other than the data, even for the servers the firewall device is basically expected to allow access only to authenticated set of users or authenticated set of devices to get inside the network and thereby preventing others from sort of accessing any part of the network either either be it in terms of either the servers or in terms of even the data on those servers.

So there are typically two types of firewalls, one which is called as an application level firewall, another which is called as a packet filtering level firewall, right?

(Refer Slide Time: 08:24)



Packet Filtering

Should arriving packet be allowed in? Departing packet let out?

- internal network connected to Internet via router firewall
- router filters packet-by-packet, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type

So packet filtering level firewall will basically be filtering the packets on in individual bases right, so I will basically have a different configurations done on my firewall device here, so let us say that I have the firewall device available as part of my network router at my edge itself.

Which is basically the one that is really connecting to my internet right, so on that firewall device I will basically have configurations specifying what kind of packets that are actually going out from my intranet to the internet should be allowed and what should be denied and similarly what kind of packets that are actually coming from the internet into my intranet should be also allowed and should be denied access right, so thereby I will basically try to have this filtering done.

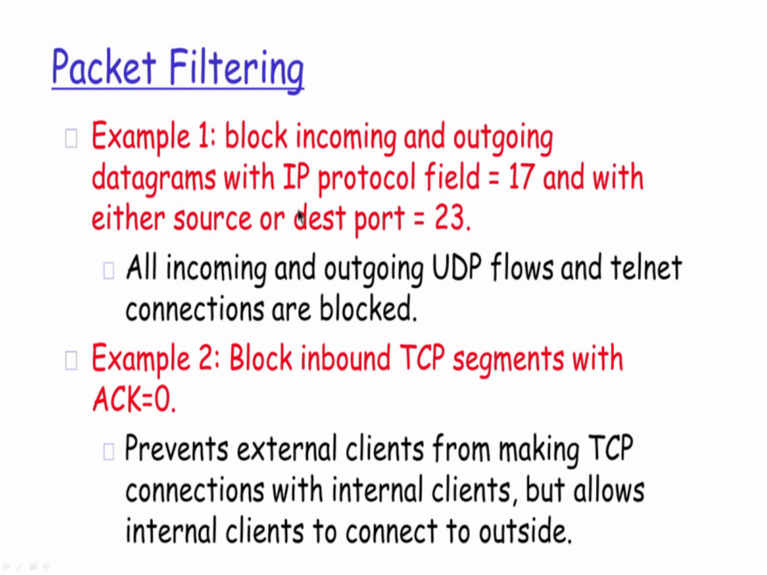
On a per packet bases wherein every packet that is actually going out or coming inside my network, so either going out of my internal network or coming inside my internal network will be subjected to these filtering rules only if the filtering rules is allowing it to be passed on the other side right, so the packet will really be sent to the other side and if if if that is not allowed or if it is expel if it has been explicitly denied the firewall is expected to silently drop the packet.

Without forwarding it to the other side, other than whichever side it basically came from right, so I could basically set it based on set these filters based on what is the source IP address of the packet, or what is the destination of the IP address or what is basically that the the source port or the destination port at my TCP or UDP level, at the transport level right, or I could basically base it on the ICMP message type, so what kind of messages can basically go out of my intranet to the internet.

And also vice versa, so for example we had actually seen a trace route application in our module, so the trace route application is actually using ICMP message and for a security reasons there will be certain firewall configurations which would have been done to sort of disable these ICMP messages from going outside the network or ICMP messages even getting responded from one part of the network to another part right.

So based on these parameters, I could basically set on my firewall a filtering mechanism to the either allow or deny on a per packet bases and that is basically the reason why we keep calling this type of a firewall as a packet filtering firewall, right?

(Refer Slide Time: 11:00)



Packet Filtering

□ Example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.

  □ All incoming and outgoing UDP flows and telnet connections are blocked.

□ Example 2: Block inbound TCP segments with ACK=0.

  □ Prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

So look at this one example so block incoming and outgoing data grams with the IP protocol field set to 17 and with either source or destination port as 23 right, so all the incoming and outgoing UDP flows.

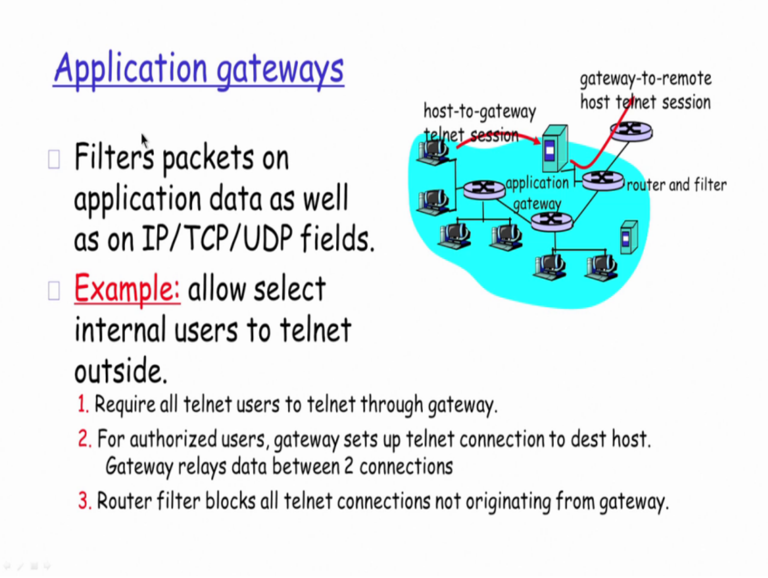
Because if the IP protocol field is set as 17 that essentially means that it is basically referring to only the the higher level protocol to the IP layer as UDP so and with the source or destination port as 23 essentially means that 23 port number is used for telnet right, so this kind of a role will basically block all incoming and outgoing UDP flows and specifically UDP flows for the telnet protocol right, so example 2 block inbound TCP segments with the act is equal to zero right.

So this basically helps the firewall to sort of prevent any kind of an external device from trying to make a TCP connection with any internal mission that is there as part of my local intranet right, so because of the fact that I am basically saying inbound TCP segment with act is equal to zero and that is basically going to come in only when I have a syn segment for the connection TCP connection establishment from the outside network to coming into an internal node inside my network.

But because of the fact that it is only telling inbound all kind of internal clients or devices can actually try establish successfully a connection to the outside world right, because specifically the the filter here is basically talking about only inbound TCP segment this is not going to sort of block all outbound TCP segment, so outbound TCP segments or inbound TCP segments is always with respect to the direction of traffic from the firewall device.

So if there is a traffic that is coming from internet into the intranet it is going to be referred to as inbound, if the traffic is going from an intranet that is my local network to the external internet it is going to be referred to as the outbound, so in this particular filter configuration that I might have on the firewall this will only block all incoming connections TCP connection request to any mission in my internal network but it will allow any kind of an external connection going out from my internal mission, any of the internal missions to anywhere outside in the internet.

(Refer Slide Time: 13:30)



Application gateways

- □ Filters packets on application data as well as on IP/TCP/UDP fields.
- □ Example: allow select internal users to telnet outside.

1. Require all telnet users to telnet through gateway.
2. For authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. Router filter blocks all telnet connections not originating from gateway.

host-to-gateway telnet session
gateway-to-remote host telnet session
application gateway
router and filter

So coming into the application gateway I would basically try to have a application gateway component for each of my applications so all kinds of traffic for that particular application will only be routed through that particular gateway component right.

So in the previous case, in the previous type of a firewall what we were really trying to do was we were actually trying to have one single firewall device which was actually doing the filtering based on the conditions for all types of packets going inside or outside right, whereas in application gateway there will be no packet filtering done on an individual packet bases but I will typically have different gateways for different applications that I might be running right.

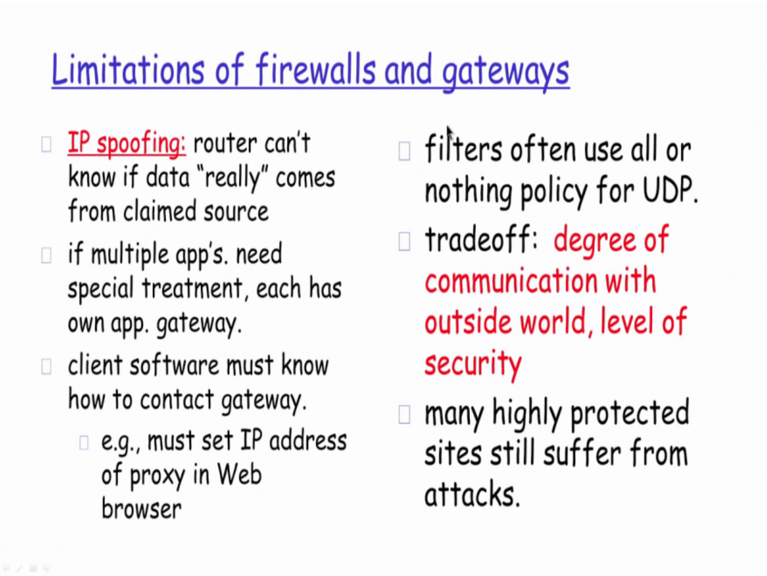
So for example if I have a http application I might have http gateway, if I have a telnet application I might have a telnet gateway, so the telnet users will all be expected to go out into the public internet right, only through that particular telnet gateway right, so any any mission on the network if it is expecting to get out to the public internet will only be able to go through this telnet application gateway and only then this router will accept the connection.

To get out onto the public internet, so if I basically try to have a a mission here in my network trying to directly go outside into the public network by trying to, if it wants for example do a telnet right, this particular router will sort of disable that because there is an application gateway firewall component that is actually setup in this particular network because of which all the the application traffic specific for that has to be routed only through one single server right.

So I could like for example have something similarly for my http protocol also and that is basically what we very commonly refer to as a as a proxy server right, so if I have a proxy server and I have the proxy server connected to my firewall, I will be able to hit multiple birds in one stone with the proxy server I will be able to have a better performance because the proxy server is typically going to cash the pages locally with the same proxy server.

I will also be able to allow and disallow certain types of users or certain types of IP addresses from going and browsing the outside network, so all these things I will be able to do with the single proxy server, so the proxy server is when I, another example of a typical application gateway where the the firewall rules will be setup on a per application bases.

(Refer Slide Time: 16:04)



Limitations of firewalls and gateways

- □ IP spoofing: router can't know if data "really" comes from claimed source
- □ if multiple app's. need special treatment, each has own app. gateway.
- □ client software must know how to contact gateway.
  - □ e.g., must set IP address of proxy in Web browser
- □ filters often use all or nothing policy for UDP.
- □ tradeoff: degree of communication with outside world, level of security
- □ many highly protected sites still suffer from attacks.

So there are certain very common limitations of firewalls and gateways also, there is a a IP spoofing done. So IP spoofing really means that the attacker is basically trying to change the IP address from the actual IP address to something else, and then try to bypass the the firewall rule maybe because the firewall is allowing certain IP addresses to be using the firewall device to be having there packets sent out in that case, if there is a spoofing of the IP address that is possibly done, there is a possibility that the router might not know the data is actually really coming from.

The the claimed source right and similarly I also will have a a requirement if I am using a gateway if I really have multiple applications that are required to be running in my internal network, all requiring a gateway firewall component, I need to actually have multiple application gateway setup right, so in that way I will also need to have the individual clients being in a position to sort of know how to actually connect to that particular gateway.

In addition to having multiple gateways installed in my network, so all these basically have create certain limitations in how effectively or how optimally these kind of firewall devices are actually used right, so there is a common trade out that I will have to typically encounter wherein the degree of communication of the outside world and the level of security is always a trade out, so the more the amount of communication I want to have with the outside world.

I will have possibly lesser in lesser level of security or I will take a hit on the performance right, so I cannot really have a very high degree of performance and at the same time expect to have hundreds of filtering rules configured on my firewall because for every packet that is actually going through the firewall all these rules are going to be checked, if all these rules are going to be checked then obviously there is going to be a hit on the performance rate.

Because that time that the packet is going to be taking for it to be actually sent out of the device is going to become that much more as the number of rules increases that needs to be checked, so there is always a certain trade of between the amount of network security that we need to have established verses the kind of performance that we would really like to have and this trade of is a very delicate balance that the network administrator typically tries to achieve.

Thank you.