Computer network security and firewall

What is the relationship between a TCP and UDP packet? Will any specific transaction usually involve both types of packets? A TCP Packet sends Information, and reports back to the sender on progress to assure that information has been sent and received. LCD on the other hand is designed more for speed after establishing a connection and is used to strive for the fastest data retrieval rate as possible, but for this type of packet, it’s less important that it reports back.

I don’t believe there will be specific transactions that involve both types of packets. But TCP is better for assuring that data Is being received completely, but UDP focuses on assuring data Is retrieved as quickly as possible. 3. How is an application layer firewall different from a packet-filtering firewall? Why is an application layer firewall sometimes called a proxy server? A packet-filtering firewall only allows “ a particular packet with a particular source, destination, and port address to enter. (POSS. P. 53) An application layer firewall is sometimes called a proxy server because It “ runs special software that acts as a proxy for a service request” It Is more to deal with outgoing connections and making connections within the DMZ zone of an organization. 4. How Is static filtering different from dynamic filtering of packets? Which is perceived to offer improved security? Static filtering works with rules that are already designated or “ developed and installed with the firewall” and only a person can change it, as software isn’t smart enough to determine if those connecting is authorized or not.

However dynamic filtering of packets recognizes unauthorized patterns or connections that are unusual and Immediately begins to block them or filter them, I believe that dynamic filtering Is perceived to offer improved security,

but unfortunately, if an attack Is made to that firewall using a DODOS attack, the firewall would probably be overloaded and not be blew to handle requests as it would keep having to add temporary IP restrictions and therefore limiting others from connecting. (POSS. P. 253) 5. What is statutes inspection?

How is state Information maintained during a network connection or transaction? Statutes Inspection keeps “ track of each network connection between Internal and external systems on a state table. ” This basically means any kind of traffic that goes through a statutes inspection firewall is monitored to where it came from and who used it. State information is maintained by looking at its state table, then refers to its access control logic to see whether it’s k to let traffic occur. 6. What is a circuit gateway, and how does it differ from the other forms of firewalls?

After reading this portion on Circuit Gateways several times, It Isn’t exactly clear to me what a circuit gateway Is, but It seems that It’s much Like setting up a VPN wealth a network to firewalls because it does no extra processing and scanning to make sure the information is k to let through. There’s already a secure connection being established between an application on the outside of the network and the inside. 7. What special function does a cache server perform? Why is this useful for larger organizations?

A cache server is a server that basically makes available frequently used pages. For example, big corporations use cache servers to make sure pages that they use to market their products are basically pre-rendered and ready to send instead of asking for a full request from a website host. It also adds

an additional layer of protection against attacks as only portions of a website can be attacked at a time. 8. Describe how the various types of firewalls interact with the network traffic at various levels of the OSI model.

Packet filtering firewalls include Static Filtering, yeoman filtering, and statutes inspection filtering these all work at the transport layer of the network. Packet filtering interacts with network traffic to confirm or deny it based on a rule set for a packet going up against a set of rules that is determined. Static filtering is up against a rule set for each packet, dynamic filtering filters packets depending on network traffic and usage limits, and statutes inspection examines packets and verifies where they are coming and going to determine via logs. . What is a hybrid firewall? A Hybrid firewall " combine the elements of other types of firewalls that is, the elements of packet filtering and proxy services, or of packet filtering and circuit gateways. " (POSS. P. 256) It's pretty nice because it takes all the network security protocols and kind of combines them in one package so a network can be improved without replacing several different firewall technologies. 10. List the five generations of firewall technology. Which generations are still in common use? SST Generation: Static packet filtering (going up against a pre-defined set of rules) 2nd Generation: Application level firewalls, which are able to be configure via applications and have he ability to manage traffic that applications make," providing intermediate services for requesters" (POSS. P. 256) 3rd Generation: Inspection firewalls: " monitor network connections between internal and external systems using tables. " (POSS. P. 256) 4th Generation: Dynamic packet-filtering firewalls, " allow only a particular packet with a particular service, destination, and port address to

enter. (POSS. P. 256) 5th Generation: A kernel proxy that evaluates packets at multiple layers, checking security as it’s passed through the firewall. There is a “ security policy that is configure into the kernel proxy as it inspects each packet. (POSS. P. 256) The generations that are in common use are pretty much all of them, but it’s more likely that application level firewalls, or kernel proxy firewalls being the ones most often used. 1 1 . How does a commercial-grade firewall appliance differ from a commercial- grade fire- wall system?

Why is this difference significant? A commercial-grade firewall appliance is a firewall that is completely independent from client computers, it runs on the firmware of a switch, and is maintained through a direct connection to the switch. Via that connection it can be configure to block and allow different kinds of traffic. A commercial grade firewall system basically runs as software on client computers which allows and prevents different kind of traffic from coming and going through a network connection.

This is a significant difference because the load of not a separate box. In order to decrease load problems from servers and other clients on a network, a commercial-grade firewall appliance is highly recommended. 12. Explain the basic technology that makes residential/SOHO firewall appliances effective in protecting a local network. Why is this usually adequate for protection? Many single office, or home office setups don’t need to have a crazy amount of retention because it’s unlikely that they would be a target of an attack verses a small home or business.

This is adequate for protection because it creates a local NAT, works as a basic almost built in firewall, and stops most known intrusions or connections internally. 13. What key features point up the superiority of residential/ SOHO firewall appliances over personal computer-based firewall software? Restrict Mac filtering, allow port forwarding, configuring ports to be on or off, and also they are easy to configure because they are usually built into a network sharing switch. 14. How do screened host architectures for firewalls differ from screened subnet firewall architectures?

Which of these offers more security for the information assets that remain on the trusted network? Screened host architectures use both packet filtering and a separate dedicated firewall, it allows packets to be screened before entering a network and accessing an internal proxy. While a screened subnet firewall architecture utilizes a DMZ as a dedicated port between the device and a single host. This helps even more with routing unauthorized network traffic, as all requests that occur within the network do not respond to outside IP addresses.

Screened subnet firewalls with a DMZ offer way more security as it is very difficult to communicate with servers in a DMZ because they are only configure to communicate on the local network. 15. What a sacrificial host? What is a bastion host? A sacrificial host is a host that works as a sole defender of a network and communicates between incoming information and works as a proxy server. The separate host that’s used to perform communication protocols on a server is called a bastion host. 16. What is a DMZ?

Is this really an appropriate name for the technology, considering the function this type of subnet performs? A DMZ works as sort of a middle ground between an entrusted network and a trusted network, usually between two firewalls. I believe it is a proper name for the technology as it helps with being an area where nobody can really do anything, unless somebody is tapped directly into the line itself. 17. What are the three questions that must be addressed when selecting a firewall for a specific organization? 1 . Which type of firewall technology offers the right balance between protection and cost for the needs of the organization? ” “ 2. What features are included in the base price? What features are available at extra cost? Are all cost factors known? ” “ 3. How easy is it to set up and configure the firewall? How accessible are the staff technicians who can competently configure the firewall? ” “ 4. Can the candidate firewall adapt to the growing network in the target organization? ” (POSS. P. 67) Paraphrased, how big is your organization, how much security will you need, how is your budget and how much do you want to be managing incoming and outgoing connections. 18. What is RADIUS? What advantage does it have over ATTACH? RADIUS or “ Authentication Dial-Len User Service” works to help allow a user to log in and work motley it first comes as a request remotely from (hopefully) an authorized worker, it the radius server to confirm or deny the request, then the yes or no signal is sent back to the remote access server and back to the client to confirm the connection request.

This is convenient because while one server can be used to work with authentication, if it ever got overloaded, the local radius server would still be accessible. Radius however adds an additional layer of security using “

encryption standards including Internet Protocol Security (Pipes) or Transport Layer Security TLS)” I personally prefer RADIUS security as it works great with a VPN and usually isn’t a problem when coming as an outbound connection through a firewall. (POSS. P. 279) 19. What is a content filter?