

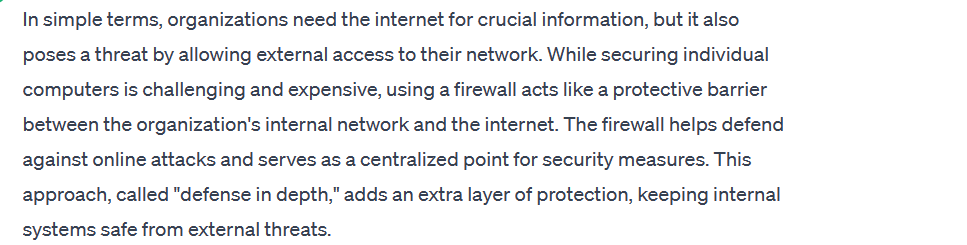
**Last Slide Image**  
Sure, the architecture you sent me is an automated enterprise security system. The system is made up of a few different parts that work together to keep your network safe from attack. Let's break it down:

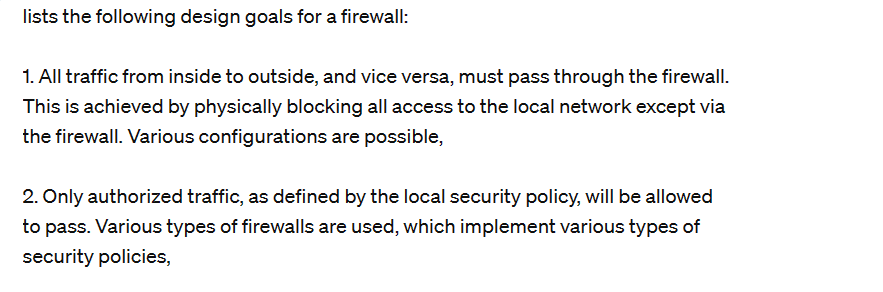
* Platform policies: These are the rules that govern how the system should behave. They're like the instructions that tell the system what to look for and what to do if it finds something suspicious.
* Events: These are things that happen on the network, like someone trying to log in or a file being downloaded. The system is constantly monitoring for events.
* Distributed detection and inference (DDI): This is the part of the system that analyzes events to see if they're suspicious. It uses a variety of techniques, such as looking for patterns in data or checking files against a list of known threats.
* Policy enforcement points (PEPs): These are the parts of the system that enforce the platform policies. They can do things like blocking traffic, quarantining files, or sending alerts to administrators.
* Adaptive feedback based policies: These are policies that are automatically adjusted based on what the system learns from the events it sees. For example, if the system sees a lot of failed login attempts from a certain IP address, it might add that IP address to a block list.

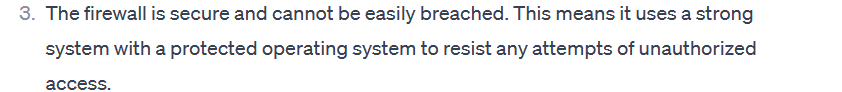
The overall idea is that the system is constantly monitoring the network for suspicious activity. If it sees something suspicious, it takes action to stop it. The system is also able to learn and adapt over time, so it can become more effective at protecting your network.

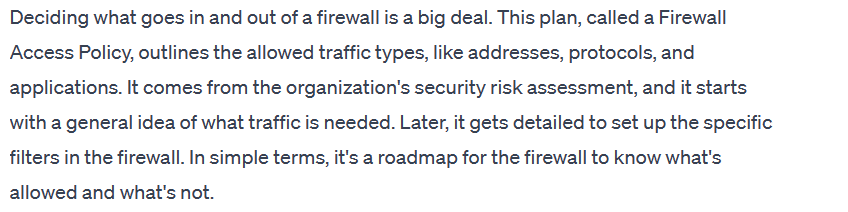
Here's an analogy to help you understand how it works: Imagine you have a security guard at your office. The security guard's job is to watch for suspicious activity and stop anyone who tries to break in. The platform policies are like the security guard's instructions. The events are like the things that happen in the office, like people coming and going. The DDI is like the security guard's eyes and ears. It helps the security guard to see and hear what's going on. The PEPs are like the security guard's hands and feet. They allow the security guard to take action to stop anything suspicious. And the adaptive feedback based policies are like the security guard's brain. They help the security guard to learn from experience and become more effective at his job.

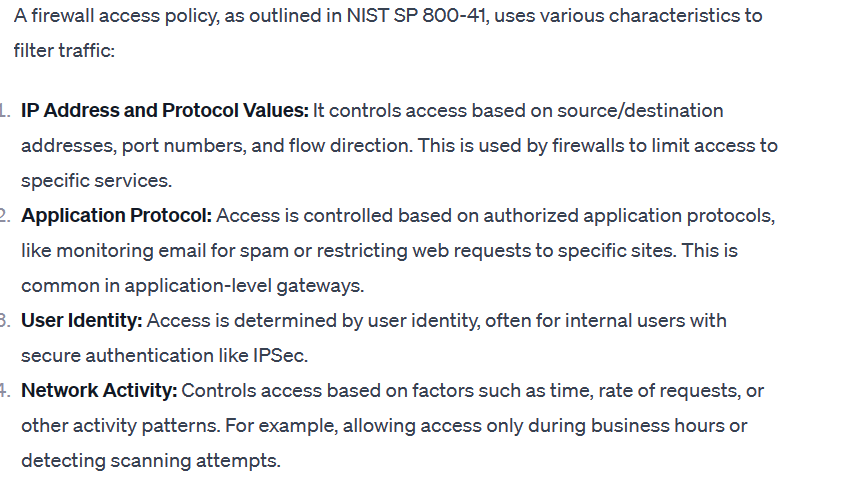
I hope this explanation is helpful! Please let me know if you have any other questions.

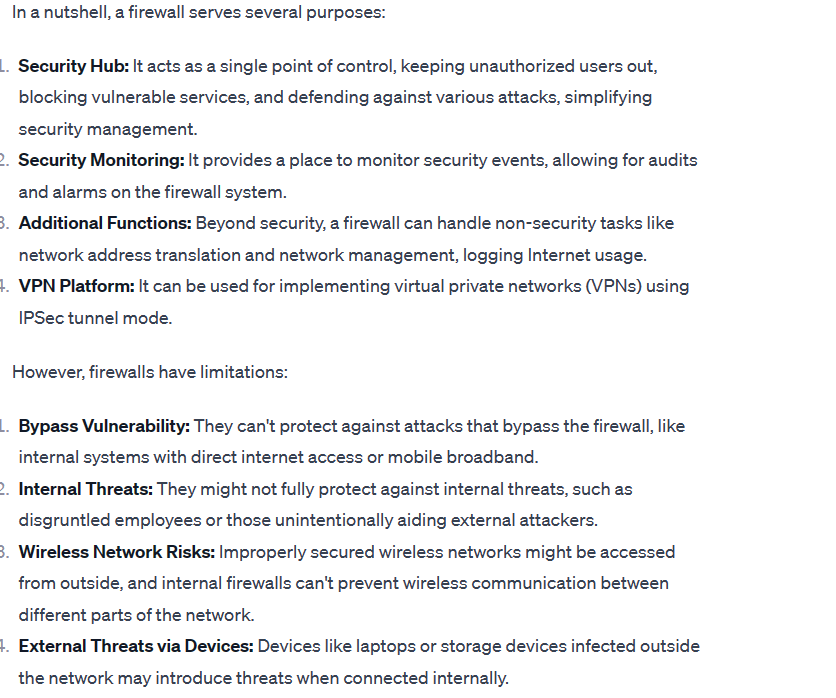
**CH 9  
  
Need of Firewall  
  
**

****

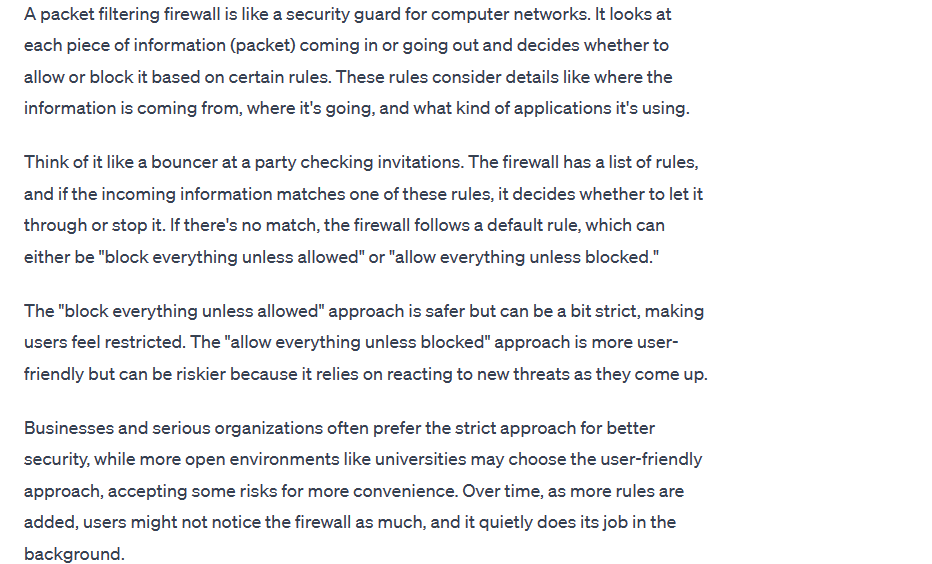
****

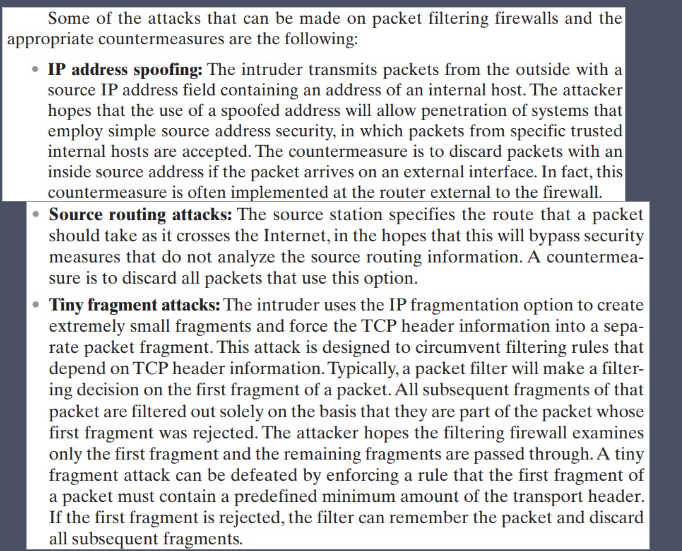
****

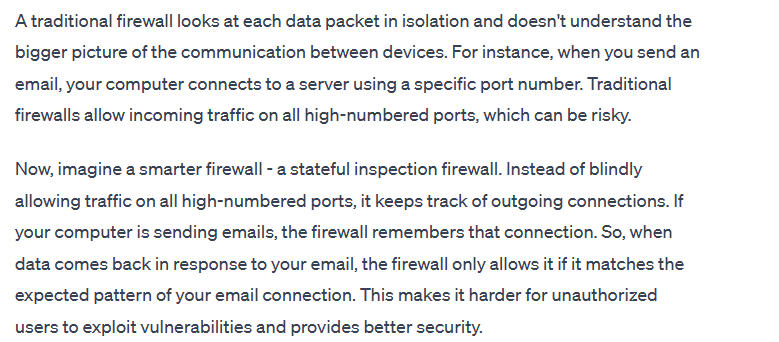
****

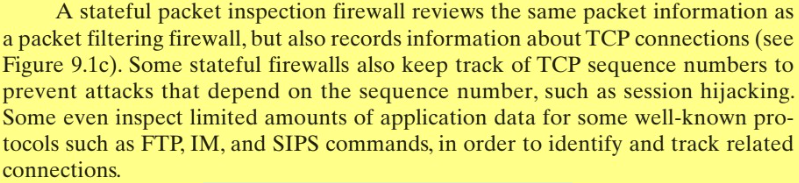
****

**1-Packet Filtering Firewall**

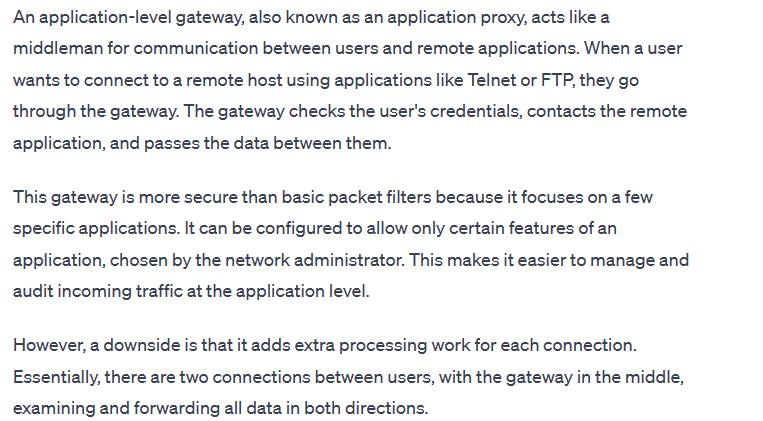
****

****

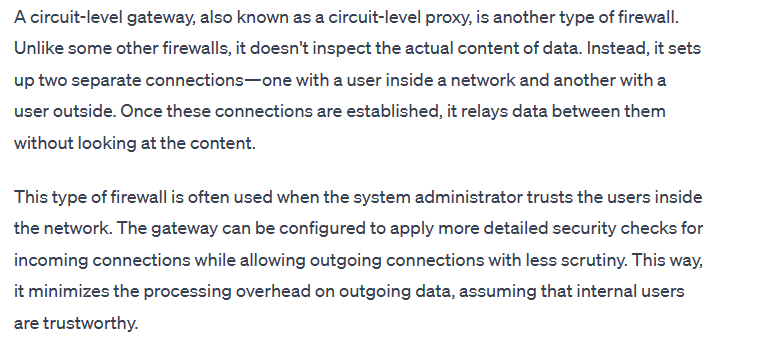
**2-State full Inspection Firewall  
  
**

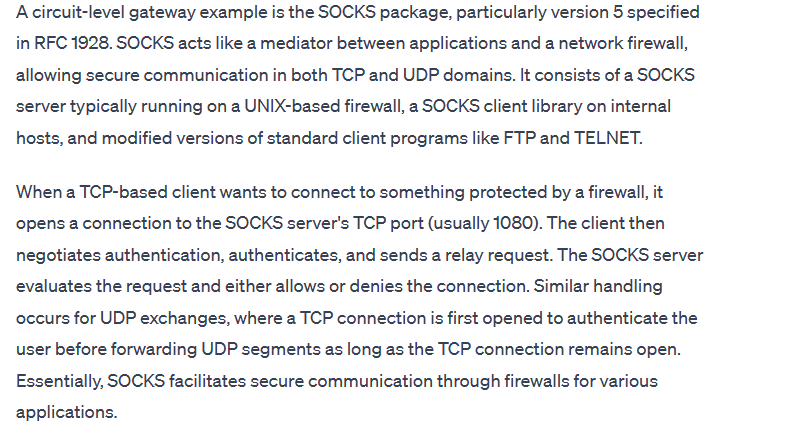
****

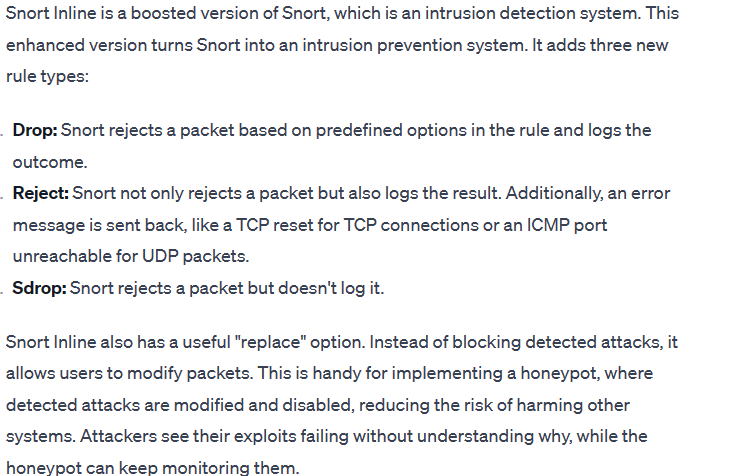
**3-APPLICATION LEVEL GATEWAY**

****

**4-CIRCUIT LEVEL GATEWAY**

****

****

****