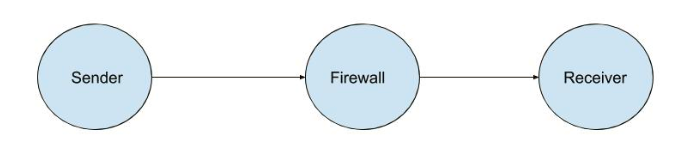
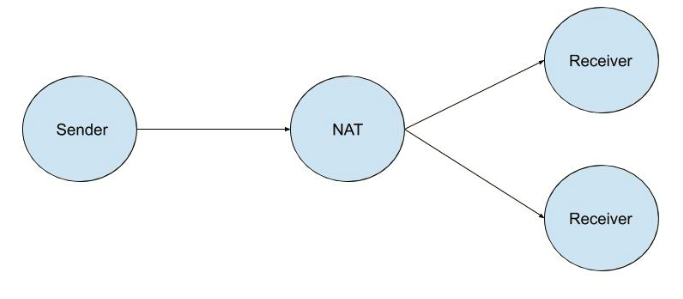
**Practical for Sessional-2**

1. Implement authentication Service. The sender sends password in encrypted format to the receiver, the receiver checks the password (after decrypting) in its database/array and replies back as success or failure.(Keys are already shared)
2. Implement authentication Service. The sender sends password in encrypted format to the receiver, the receiver checks the password (after decrypting and applying hash) in its database/array and replies back as success or failure. (Note: Here the password is stored as hash in database).
3. Implement a firewall that behaves like forwarder. It does not forward the packet that contains the word "terrorist".



1. Implement NAT functionality. The NAT works like forwarder, that will forward to appropriate receiver.



1. **Key Distribution**

Implement a program to demonstrate the functioning of a KDC. There are three entities: sender, receiver and KDC. Assume that Sender and Receiver have already established their own individual permanent secret keys with KDC. The sender requests the KDC to issue a session key to communicate with receiver. The KDC is supposed to give session key information to sender in a secure way. The same session key is also to be communicated to the receiver securely. Use a suitable protocol to achieve the above functionality.

**Hint:** KDC sends the following items to sender: 1. session key, 2. identity of sender, identity of receiver, session key. Items in 2 are encrypted by KDC using permanent secret key of receiver. Both items 1 and 2 are bundled together and encrypted using permanent key of sender and transmitted to sender by KDC. The sender decrypts the bundled items 1 and 2 using his permanent secret key. The he sends the items in no. 2 to receiver. Receiver decrypts them using his own permanent secret key and hence, gets the following information: a) identity of sender b) identity of receiver c) session key