CS253 HW6

Q1

Indicate which packets are permitted or denied and which rule is used in each case:
Permit, RuleA; Permit, RuleB; Permit, RuleC; Permit, RuleD.

Will the attack succeed? Give details:
The attack could succeed because rules B and D allow the connections where both ends are using ports above 1023.

Describe the change:
Now the firewall also restrict the src Port.

Apply this new rule set to the same six packets of the preceding problem. Indicate which packets are permitted or denied and which rule is used in each case:
Permit, RuleA; Permit, RuleB; Permit, RuleC; Permit, RuleD; Deny, RuleE; Deny, RuleE.

Q2

$$
\begin{aligned}
P(not\_attack|alarm) &= \frac{P(alarm|not\_attack) \times P(not\_attack)}{P(alarm|not\_attack) \times P(not\_attack) + P(alarm|attack) \times P(attack)} \\
&= \frac{0.1 \times 0.99}{0.1 \times 0.99 + 0.9 \times 0.01} \\
&\approx 91.67\%
\end{aligned}
$$