QUIZ

Lecture 2

Question 1

- What is the advantage of anomaly-based intrusion detection versus the signature-based intrusion detection?

Answer 1

- The accuracy of **anomaly-based detection** highly depends on the statistical tool/method used. May require some data pre-processing and some more time for the analysis, but the system might “learn” by itself. Besides that, there is a false-positive / false-negative trade-off that must be tolerated.

- **Signature-based detection** is less flexible, but can be ”faster”. Unfortunately, it is limited by the specific signatures that are available (can’t deal with new threats).

Question 2

- Is **firewall** a **preventive**, **detective**, or a **corrective** security control?

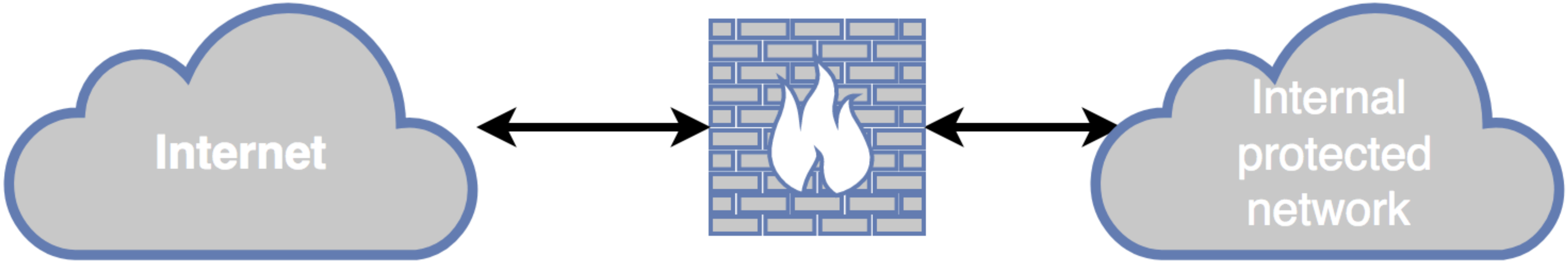
- Can you give an example of **Security Dilemma 1** (users are not experts) concerning **firewalls**?

- Can you give an example of **Security Dilemma 2** (security vs. usability) concerning **firewalls**?

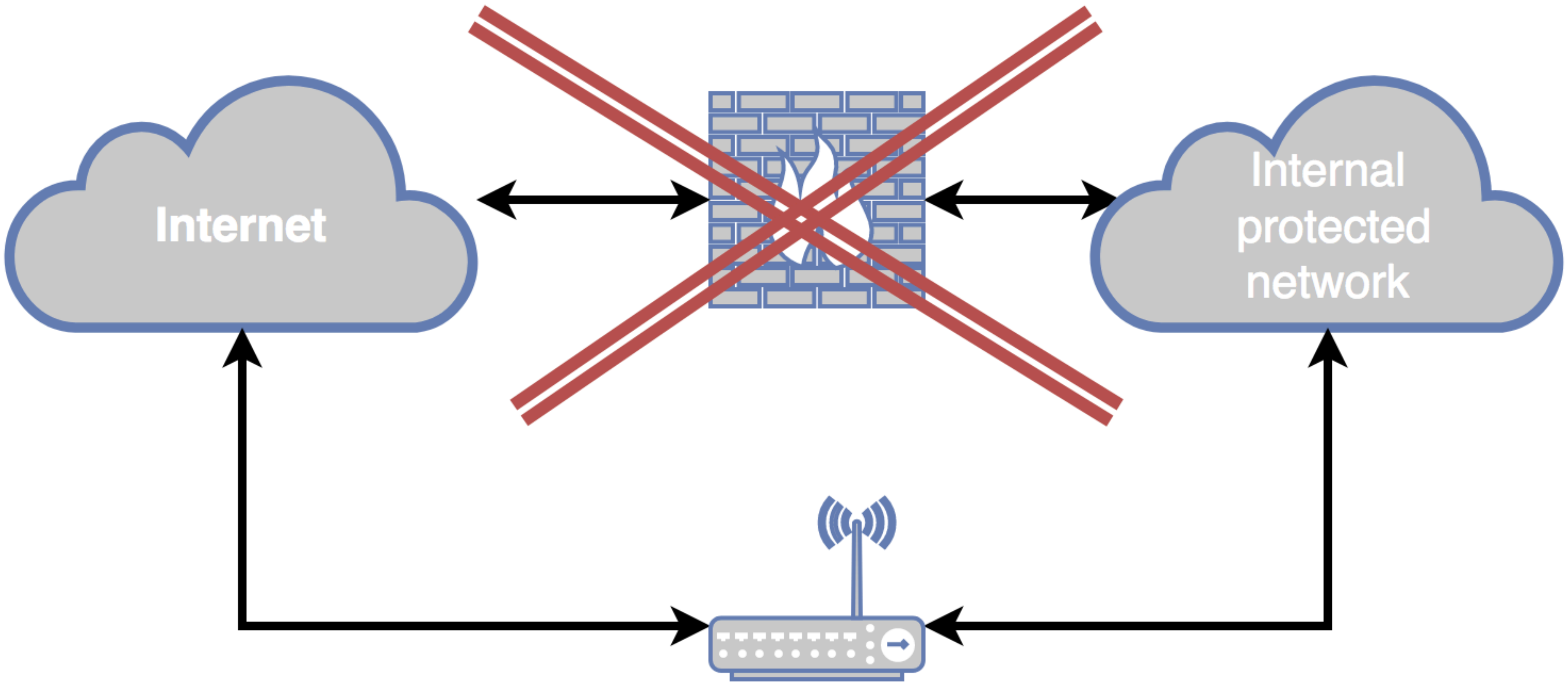
- What are the **differences** between **packet filtering** and **application-specific filtering**?

Answer 2.1

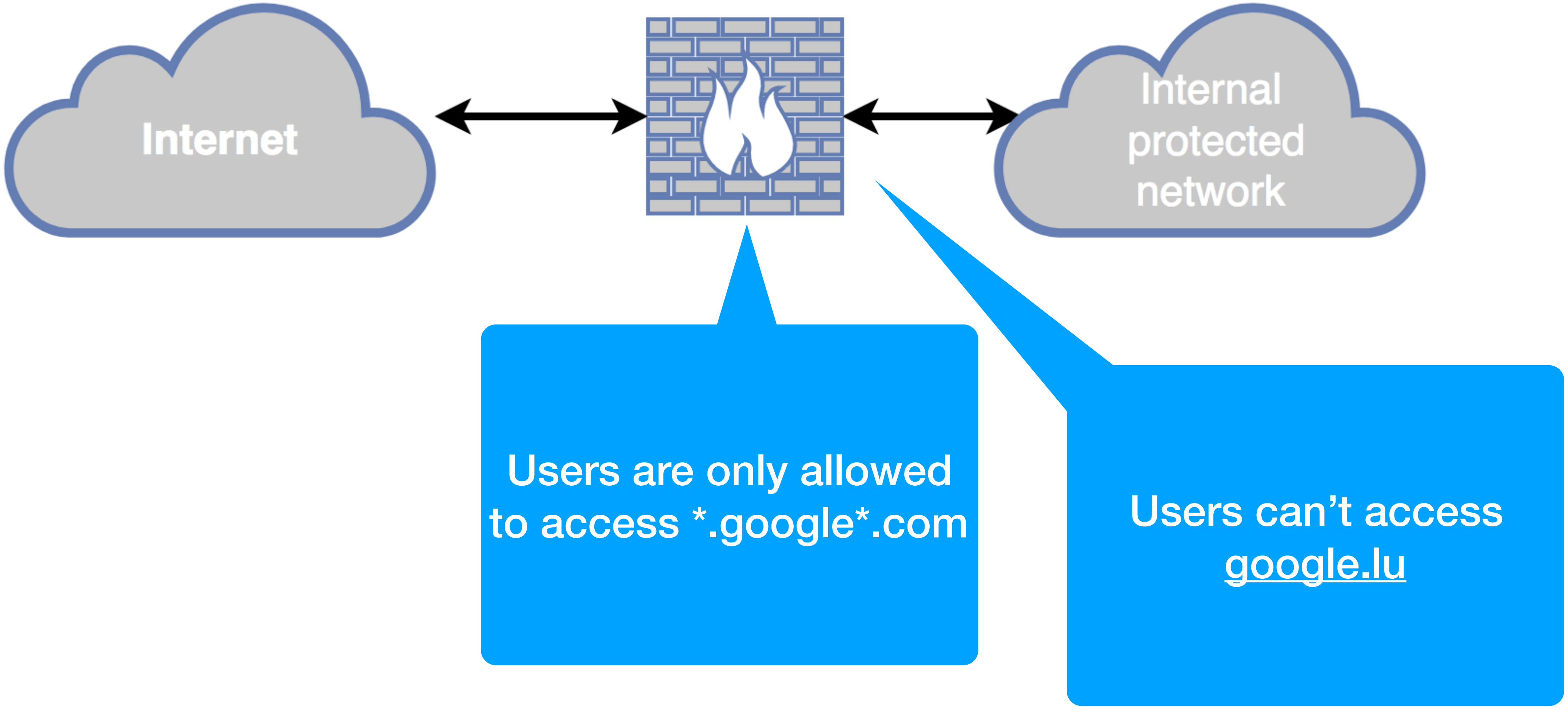
- A firewall is a **preventive** security control.



Answer 2.2



Answer 2.3



Users are only allowed to access *.google*.com

Users can’t access google.lu

Question 3

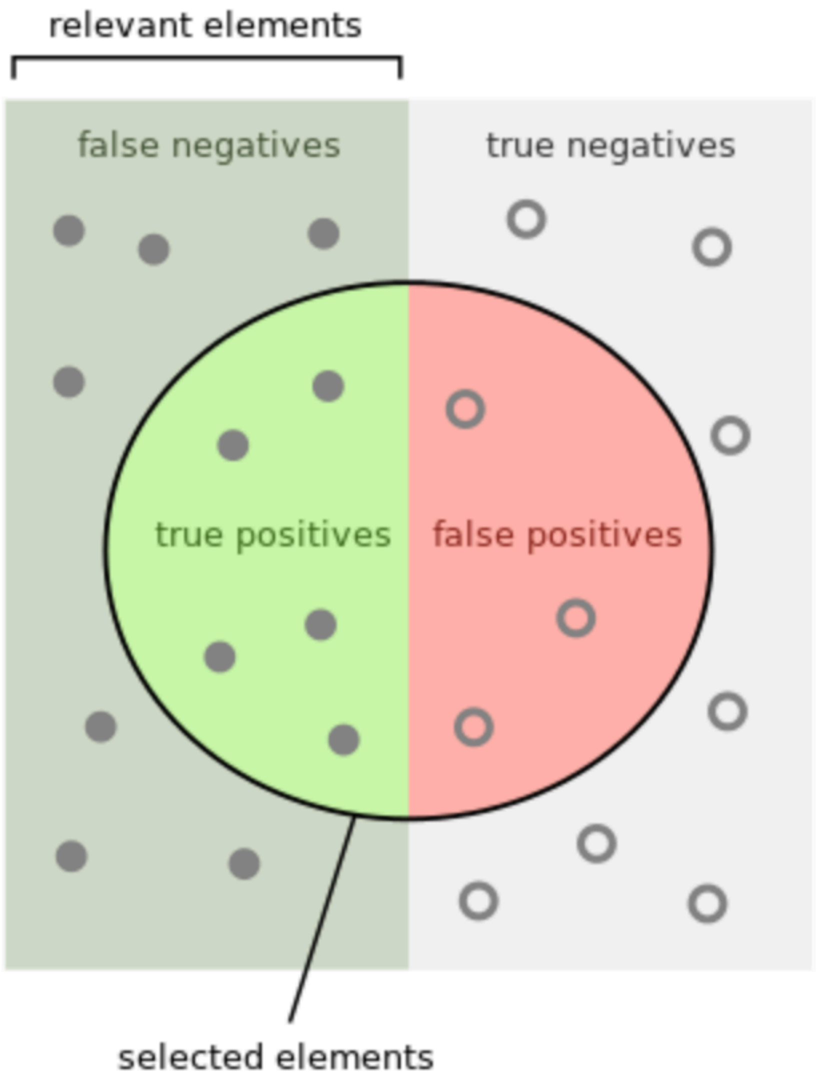
- Suppose we have a spam filter that has 98% chance of correctly classifying a spam message, and 98% chance of correctly classifying a non-spam message. Assume we have 1 spam email out of every 1,000 emails, and the filter has “seen” 100,000 emails already.
- How many emails were classified as spam?
- How many non-spam emails were classified as spam? (false-positives)
- How many spam emails were classified as non-spam? (false-negatives)
- Would you rather increase to 100% the chance of correctly classifying spam, or the chance of correctly classifying non-spam?

Answer 3.1

- **TP_{gt}**: 100000 / 1000 = 100
- **TN_{gt}**: 100000 - 100 = 99900
- Out of 99900 non-spam, **2096 are classified as spam**
  - 98% of TP_{gt} + 2% of TN_{gt}
  - 100 * 0.98 + (100000 - 100) * 0.02 = 98 + 1998

Answer 3.2

- **TP:** 98
  - 98% of TP_{gt} = 100 * 0.98
- **FP:** 1998
  - 2% of TN_{gt} = 0.02 * 99900
- **FN:** 2
  - 2% of TP_{gt} = 0.02 * 100
- **TN:** 97902
  - #Messages - (FN + TP + FP) = 100000 - (2 + 1998 + 98)



Answer 3.3

- Maybe it’s better to increase the amount of TP to 100%, so that we get 0 FP instead of 1998 and still only 2 FN (but if the ratio of spam messages will change, it might be not a good idea)