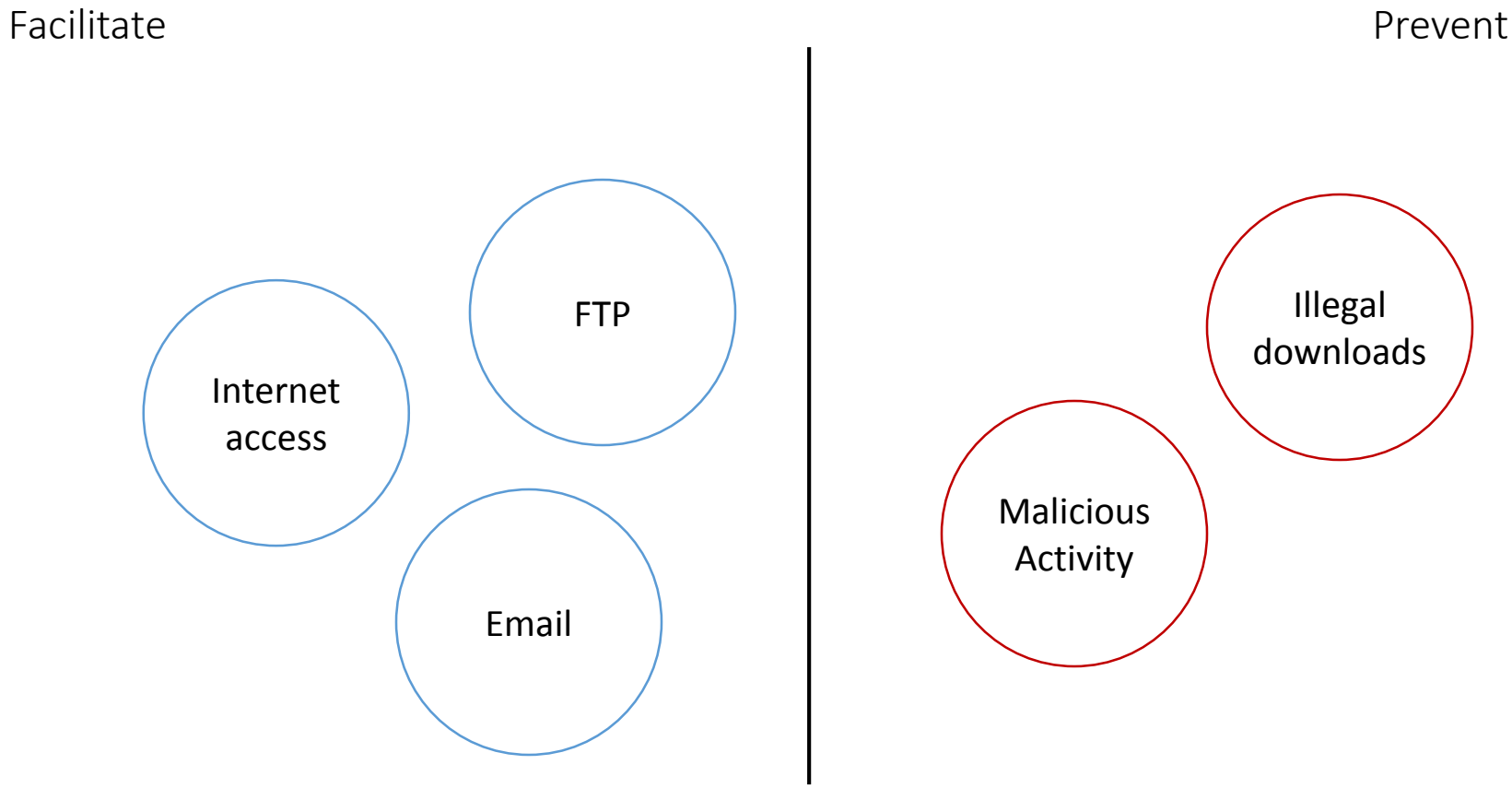
Formal Argumentation for Security Policy Maintenance

How to Maintain Policies

- Possible Anomalies
  - Conflict
  - Redundancy
- Challenge
  - Maintenance
- Solution
  - Capture design rationale

Firewalls as an Example



Technical Challenge

- Security policies involve
  - Complex interdependencies
  - Conflicting user requirements

Proposal

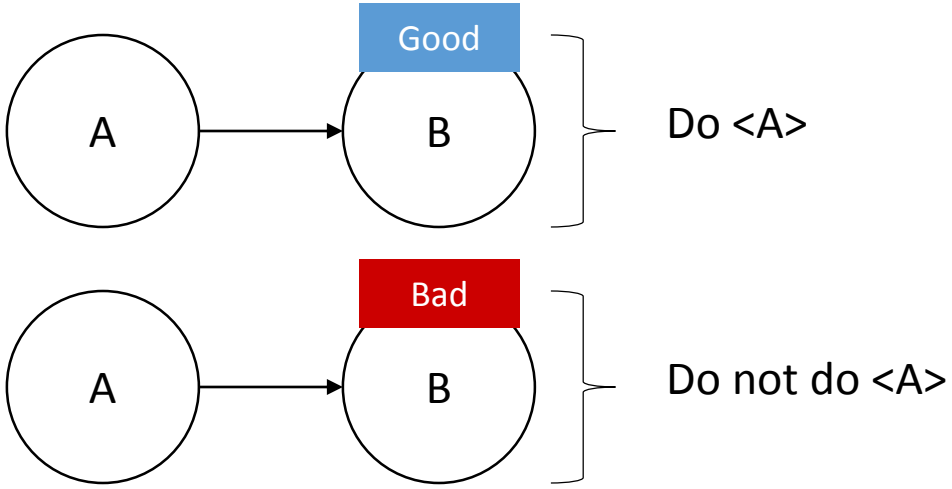
- Apply argumentation to
  - Capture design rationale
  - Reason about policies

Argumentation Schemes and Critical Questions

- Schemes
  - Patterns for constructing arguments
  - Represent inference structure of an argument
- Critical questions
  - Guide development of an argument

Argument by Consequence

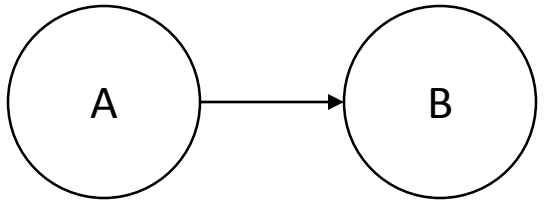
If <A> is brought then good (or bad) consequence <B> will occur. Therefore, <A> should (or should not) be brought about.



Critical Questions

Scheme: Argument by Consequence

- How strong is the likelihood of consequence?
- What evidence supports the claim?
- Are there other opposite consequence?



Argument From Position To Know

- Major Premise: Source a is in position to know about things in a certain subject domain S containing proposition A
- Minor Premise: a asserts that A is true (false)
- Conclusion: A is true (false)

Critical Questions

- CQ1: Is a in position to know whether A is true (false)?
- CQ2: Is a an honest (trustworthy, reliable) source?
- CQ3: Did a assert that A is true (false)?

Argument From Composition

- Premise: All the parts of X have property Y
- Conclusion: Therefore, X has property Y

Critical Questions

- Is property Y compositionally hereditary with regard to aggregate X (when X[the whole] has property Y, then every part that composes X has property Y)?

Argument From Division

- Premise: X has property Y
- Conclusion: Therefore, all the parts of X have property Y

Critical Questions

- Is property Y divisionally hereditary with regard to aggregate X (when every part that composes X has property Y, then X [the whole] has property Y)?

Argument by Practical Reasoning

- Major Premise: I have a goal G
- Minor Premise: Carrying out this action A is means to realize G
- Conclusion: Therefore, I ought to carry out this action A

Critical Questions

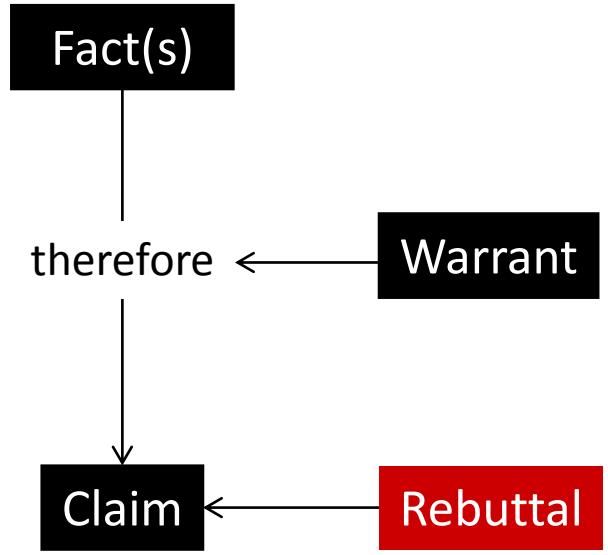
- CQ1: What other goals that I have that might conflict with G should be considered?
- CQ2: What alternative actions to my bringing about A that would also bring about G should be considered?
- CQ3: Among bringing about A and these alternative actions, which is arguably the most efficient?
- CQ4: What grounds are there for arguing that it is practically possible for me to bring about A?
- CQ5: What consequences of my bringing about A should also be taken into account?

Argument From Goal

- Major Premise: Doing act A contributes to goal G
- Minor Premise: Person P has goal G
- Conclusion: Therefore, person P should do act A

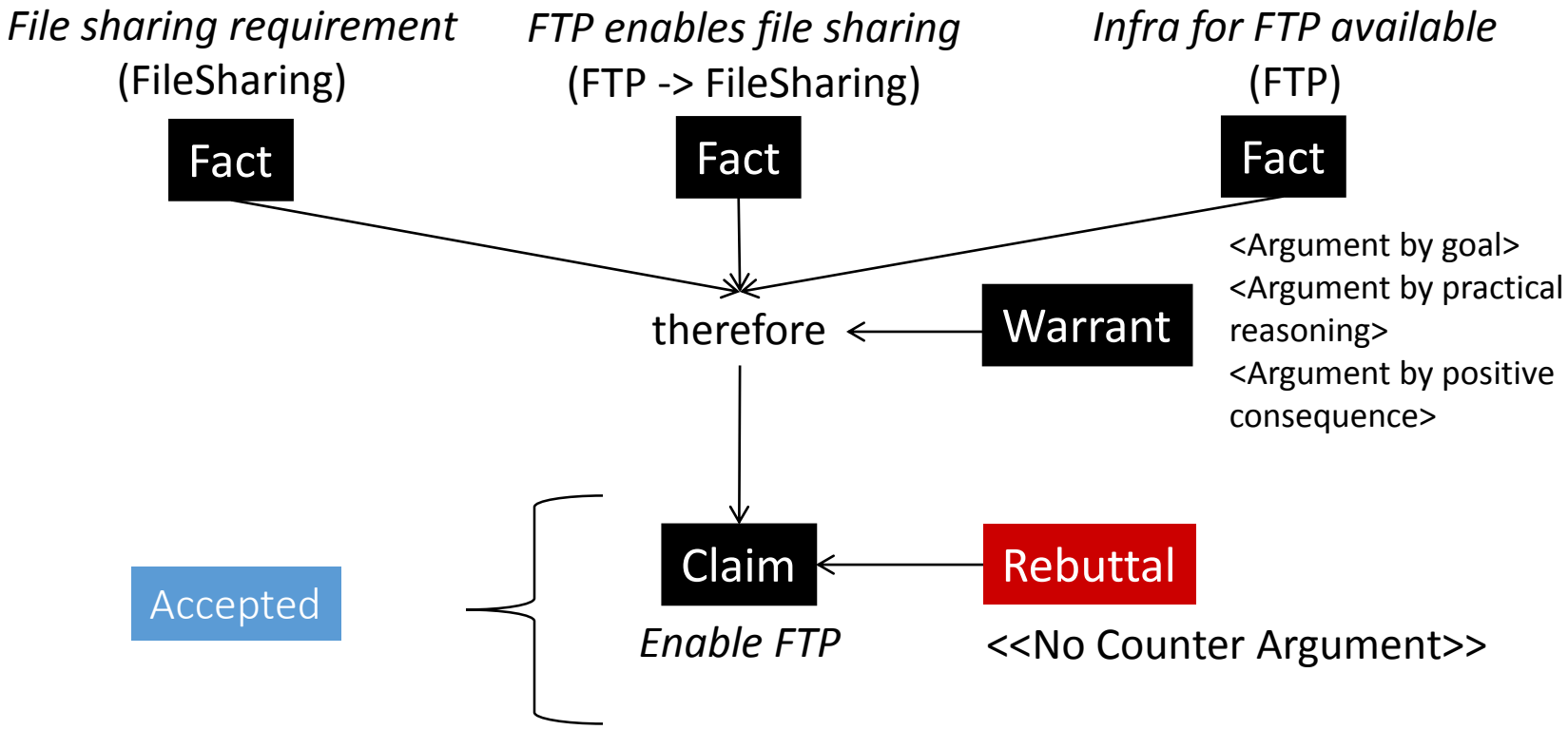
Argumentation
Toulmin's Model

- Fact
  - Data about the topic
- Warrant
  - Reasoning that connects Fact(s) and the Claim
- Claim
  - Conclusion of an argument
- Rebuttal
  - Statements recognizing the restrictions to which the claim may legitimately be applied.

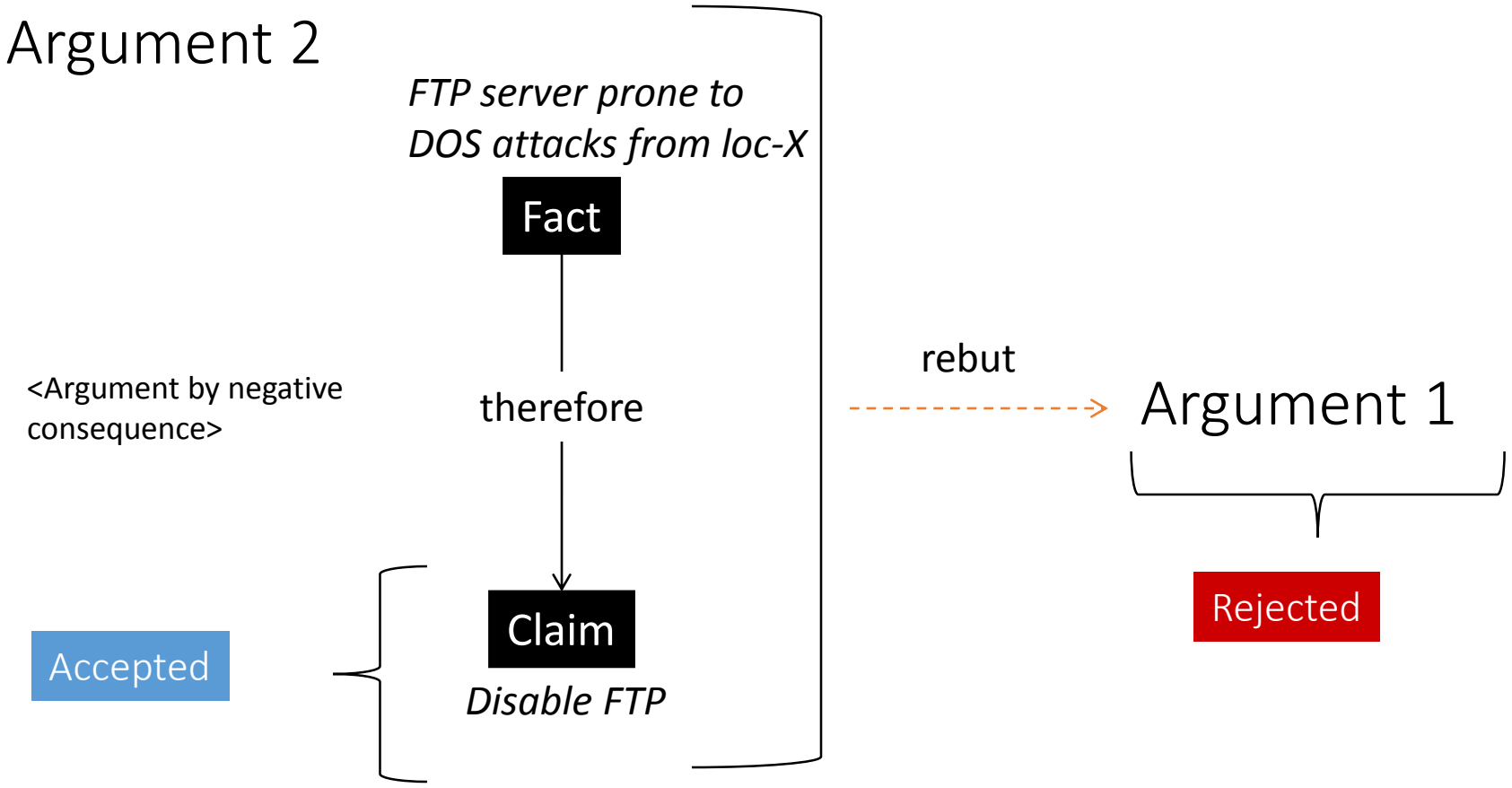


Argument for a Policy

Argument 1

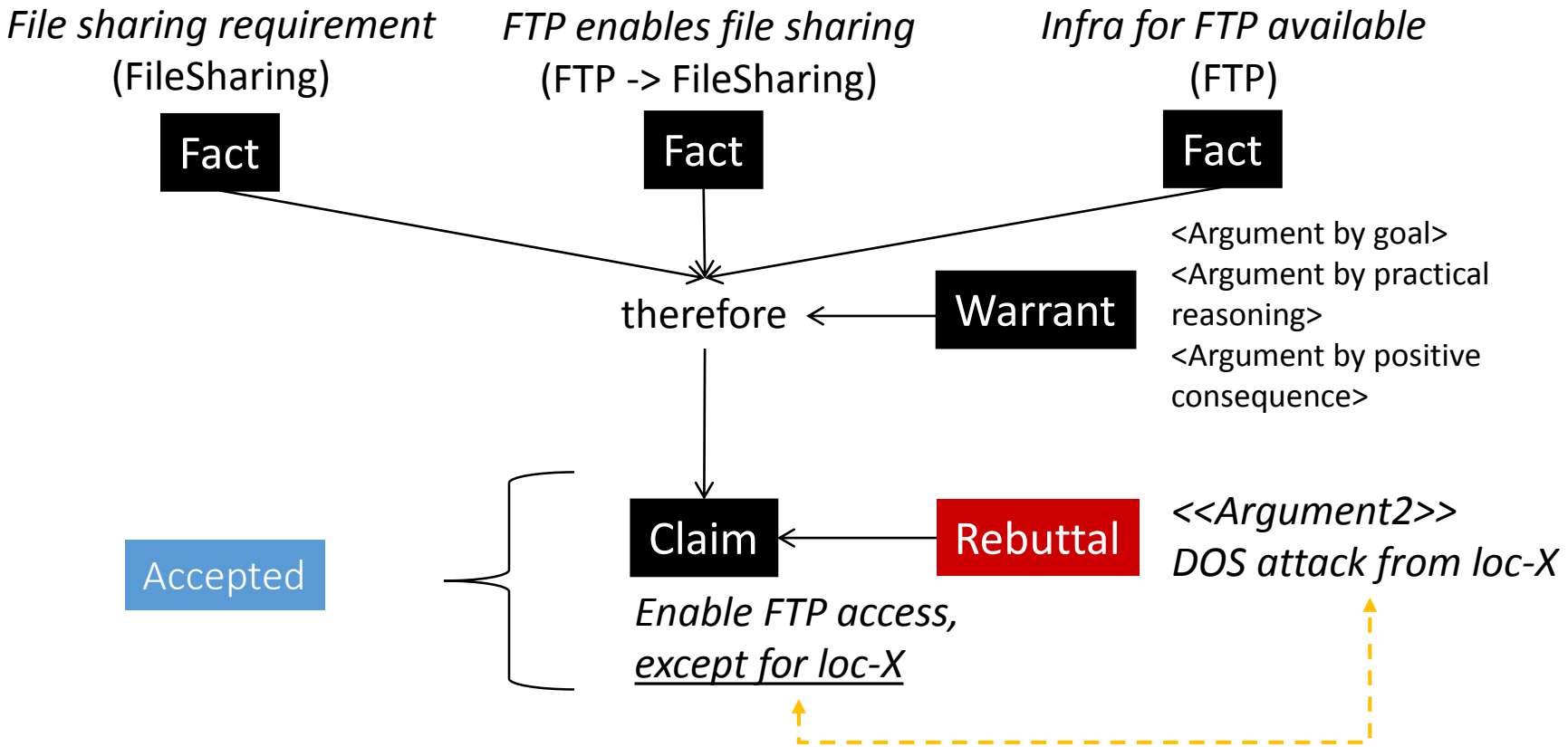


Maintenance via Argumentation



Maintenance (2)

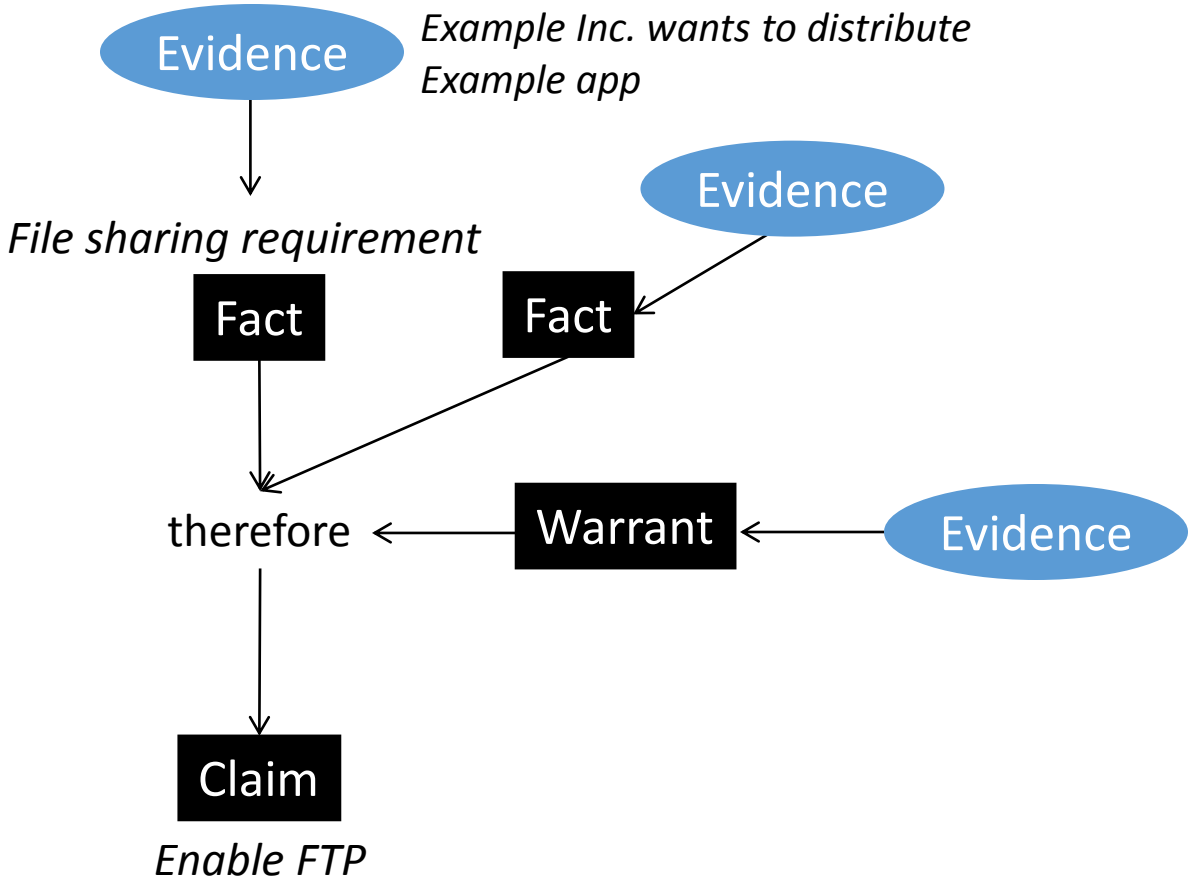
Argument 3



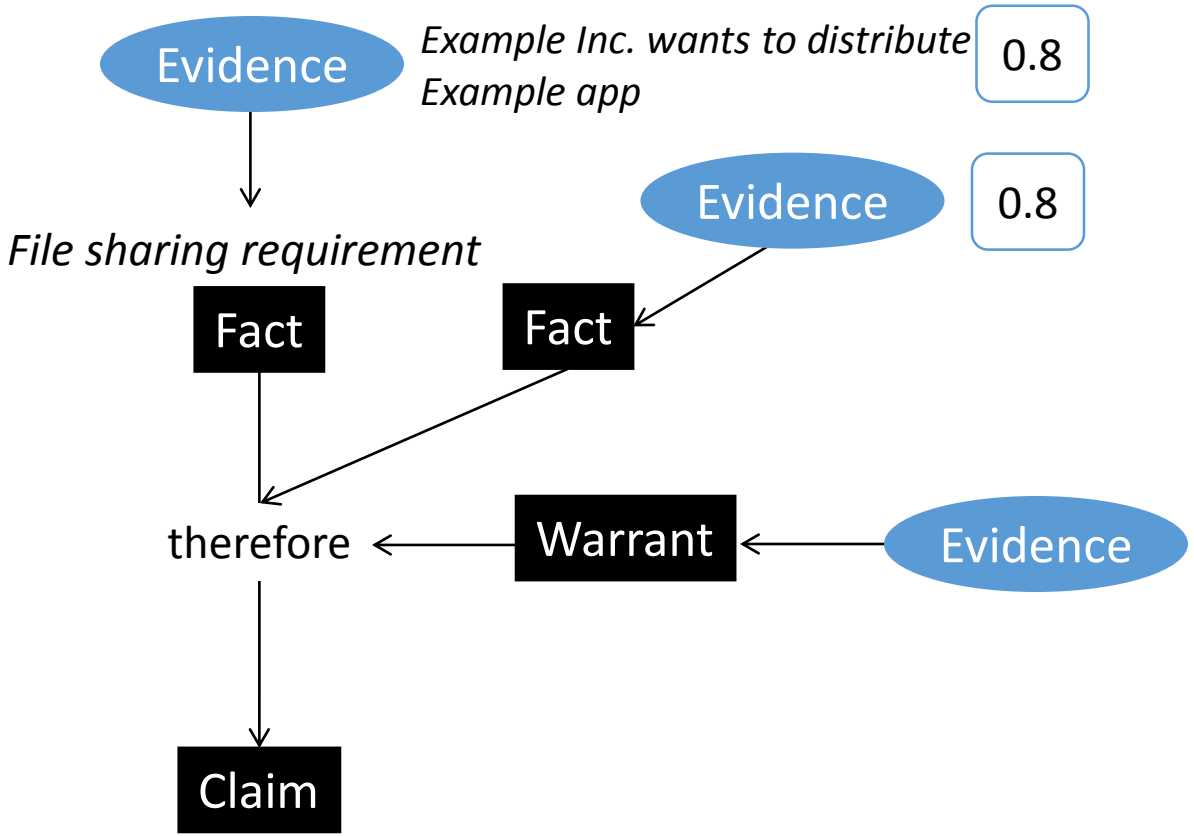
Evidence underlying Policies

#	Evidence
1	Example App needs to be distributed via FTP
2	Multiple DOS attacks on FTP server in last 10 days
3	…
4	…
5	
6	
7	

Evidence in Argumentation

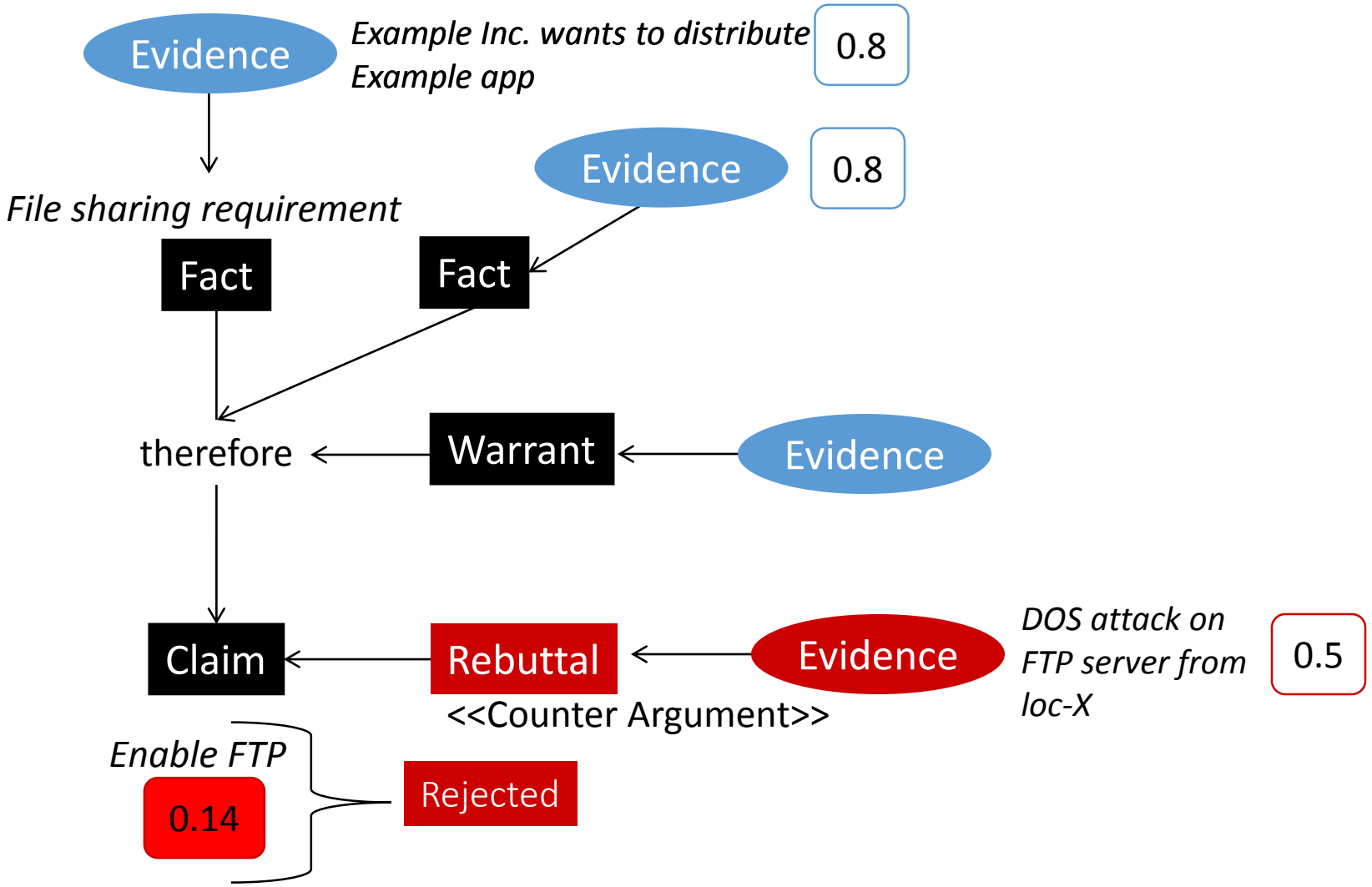


Associating Strength Value with Evidence

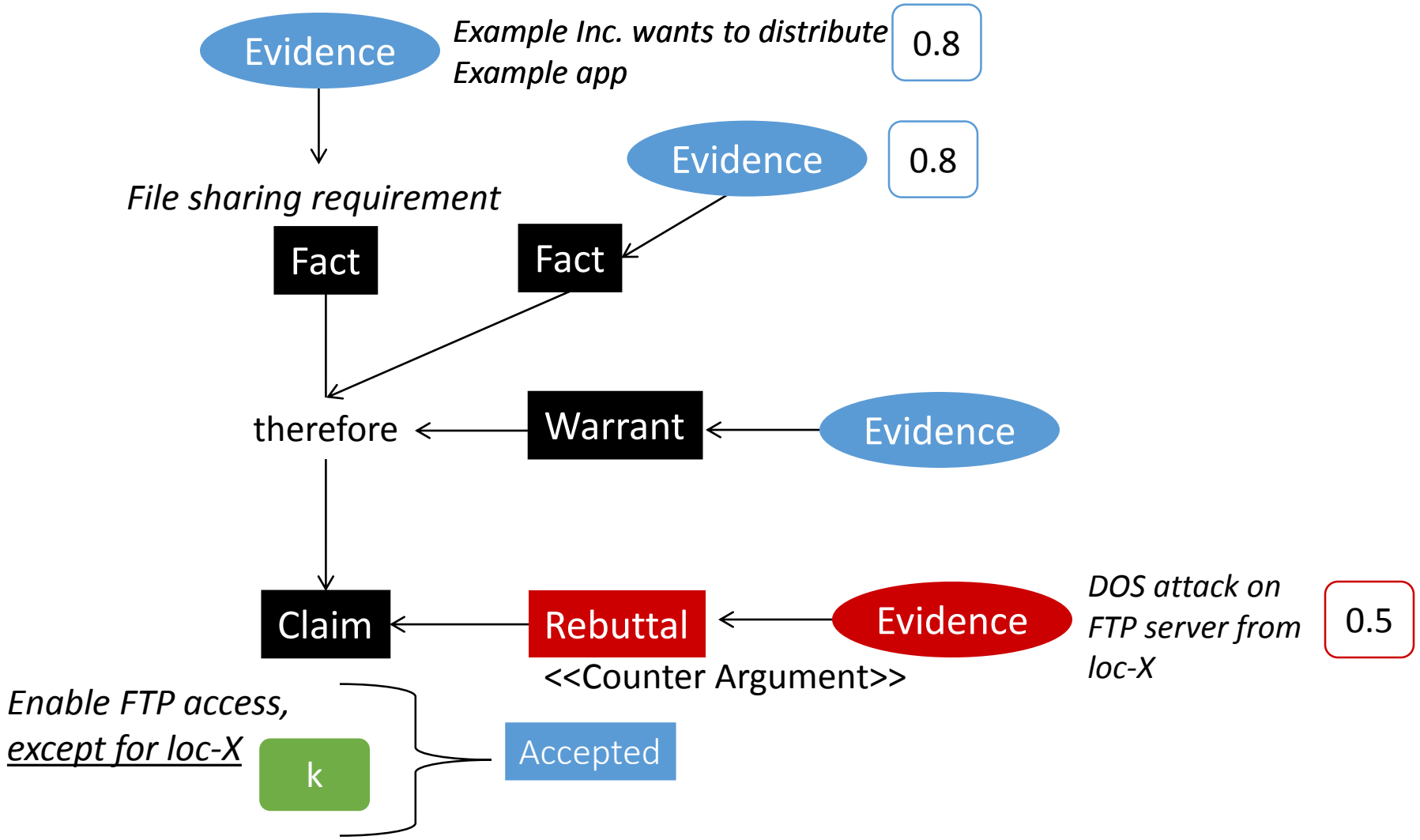


Accept claim if computed strength of claim is greater than a threshold *k*

Maintenance via Evidence in Argumentation



Maintenance via Evidence (2)



Benefits

- Rule ordering not a concern
- Reasons underlying the decision clearly visible
- Reasoning about policies easier
- Reduced uncertainty and improved completeness